PELS RIJCKEN

Landsadvocaat

Advies

voor	[redacted] (de Staat der Nederlanden (ministerie BZK))
van	[redacted] (kantoor landsadvocaat)
datum	10 oktober 2023
inzake	Gebruik generatieve AI-tools
zaaknr	11020863

Samenvatting en aanbevelingen

Privacyrecht

De GenAI markt heeft pas sinds kort de aandacht van privacytoezichthouders in Europa. Het eerste onderzoek van Garante per la protezione dei dati personali, de Italiaanse toezichthouder voor gegevensbescherming (hierna: "Garante") naar OpenAI leert ons al dat de naleving van de AVG bij de ontwikkeling van GenAI niet altijd de hoogste prioriteit heeft gehad.[1]

Niettemin, zijn er geen beginselen of vereisten uit de AVG die fundamenteel in de weg staan aan de ontwikkeling en het gebruik van GenAI. Zo kan onder voorwaarden de ontwikkelaar van een GenAI-model een geslaagd beroep doen op artikel 6, eerste lid, onder f, AVG, voor het verwerken van trainingsdata, en artikel 6, eerste lid, onder a, AVG of artikel 6, eerste lid, onder b, AVG voor het genereren van persoonsgegevens door GenAI.

De vereisten uit de AVG vormen wel een uitdaging voor de ontwikkelaars en aanbieders van GenAI. Het informeren van betrokkenen, het naleven van dataminimalisatie, het waarborgen van de juistheid van de gegevens, en de uitvoering van de rechten van betrokkenen, zijn belangrijke horden die genomen moeten worden. Enkel door substantiële investeringen in technische en organisatorische maatregelen,

[1] Garante, ChatGPT: OpenAI reinstates service in Italy with enhanced transparency and rights for european users and non-users, 28 april 2023; https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9881490#english

kunnen deze vereisten uit de AVG ook daadwerkelijk worden nageleefd. Bij het gebruik van GenAI-toepassingen door medewerkers van de Staat zal dan ook in het bijzonder moet worden gelet op de inspanning van de betreffende GenAI-aanbieder op dit gebied. In de annex bij dit advies zijn daartoe handvatten opgenomen.

Ondanks dat GenAI in beginsel kan voldoen aan de eisen uit de AVG, bestaan er ook enkele belangrijke juridische grenzen aan het gebruik van GenAI door medewerkers van de Staat. Zo zal er in de meeste gevallen geen verwerkingsgrondslag aanwijsbaar zijn voor de invoer van persoonsgegevens door medewerkers van de Staat bij het gebruik van een GenAI-toepassing. Ook het verwerken van bijzondere persoonsgegevens tijdens de training van een GenAI-model, maar ook bij het gebruik van een GenAI-toepassing kent juridische risico's. Zo is het slechts in een beperkt aantal gevallen denkbaar dat bij de ontwikkeling van een GenAI-model een geslaagd beroep kan worden gedaan op een van de uitzonderingen of doorbrekingsgronden op het verwerkingsverbod voor bijzondere persoonsgegevens. Ook bij het gebruik van GenAI lijken er weinig tot geen uitzonderingen of doorbrekingsgronden zijn waarvan een medewerker van de Staat gebruik kan maken om bijzondere persoonsgegevens te verwerken.

Auteursrecht

Het gebruik van GenAI door medewerkers van de Staat is, vanuit het auteursrecht gezien, niet per definitie onrechtmatig. Tegelijkertijd komt het gebruik ervan door medewerkers van de Staat niet zonder auteursrechtelijke risico's. Het is onduidelijk of ontwikkelaars van GenAI-toepassingen voldoende rekening houden met de rechten van auteurs wiens werken zij bij de ontwikkeling van hun diensten gebruiken. Enerzijds omdat ontwikkelaars op dit moment niet transparant zijn over de vraag welke auteursrechtelijke werken zij bij het trainen van dergelijk toepassingen wel of niet van internet (of uit andere bronnen) 'scrapen', en anderzijds omdat in de rechtspraak nog niet expliciet is geoordeeld over de vraag of en in welke vorm scraping ten behoeve van GenAI auteursrechtelijk gezien toelaatbaar is.

Voor de Staat hoeft dit niet *per definitie* te betekenen dat gebruik van een GenAI-toepassingen (door een medewerker) tot auteursrechtinbreuk leidt, al is dat risico in ieder geval in theorie wél aanwezig, en wordt dat risico bovendien vergroot door het feit dat aanbieders van veel toepassingen aansprakelijkheid in hun (standaard) algemene voorwaarden nagenoeg volledig uitsluiten.

Een tweede risico schuilt daarnaast in het feit dat de output van een GenAI-toepassing auteursrechtelijk gezien inbreuk kan maken op het werk van een (eerdere) auteur, bijvoorbeeld een auteur wiens werk ooit aan de ontwikkeling van het GenAI-model ten grondslag heeft gelegen. De precieze omvang van dit risico is nu voor eindgebruikers (en dus ook de Staat) niet goed in te schatten, al was het maar omdat aanbieders van GenAI-toepassingen op dit moment (nog) niet kenbaar (hoeven te) maken welke

auteursrechtelijke werken zij bij de ontwikkeling van hun tools precies gebuikt hebben. De AI-Act kan daar verandering in gaan brengen, maar is nu nog niet van toepassing.

Aanbevelingen
Gelet op het voorgaande bevelen wij aan:

- Geen gebruik te maken van online beschikbare GenAI-toepassingen in afwachting van nadere richtsnoeren of handvatten van bevoegde toezichthouders (bijv. EDPB en AP), en/of aanvullende regelgeving.
- Of in elk geval, slechts onder strikte voorwaarden gebruik te laten maken van online beschikbare GenAI-toepassingen, waarbij de invoer van persoonsgegevens en/of vertrouwelijke informatie technisch en organisatorisch uitgesloten is.
- Althans slechts gebruik mag worden gemaakt van (specifieke) online beschikbare GenAI-toepassingen die de bijkomende (juridische) risico's uitsluiten.

1 Uw verzoek

1.1 U stelde ons, kort gezegd, de volgende vraag:

> *Is de online beschikbare generatieve AI (bijvoorbeeld ChatGPT voor tekst of Midjourney voor afbeeldingen) door Rijksoverheidsorganisaties of in opdracht van Rijksoverheidsorganisaties juridisch mogelijk gezien de AVG, de Auteurswet en (eventuele) andere vigerende wetgeving?*

1.2 Onze beantwoording treft u hieronder aan.

1.3 Mede gelet op de korte termijn waarbinnen dit advies tot stand is gekomen, en hetgeen wij in ons overleg van 5 september 2023 bespraken, zijn wij in onze advisering uitgegaan van de werkhypothese dat het specifieke gebruik van GenAI-toepassingen door medewerkers dat de Staat op dit moment verkent en (binnen bepaalde grenzen) overweegt, zich niet uitstrekt tot activiteiten die direct raken aan de kern van het overheidshandelen. Op dergelijke vormen van gebruik heeft dit advies ook geen betrekking.

> Met andere woorden: wij hebben bij het opstellen van dit advies vooral 'kantoor gerelateerde' toepassingen voor ogen gehad, zoals (bijvoorbeeld) het opzoeken van informatie, het genereren van afbeeldingen ten behoeve van presentaties en/of het verbeteren van zelfstandig opgestelde teksten. De vraag naar toelaatbaarheid van de inzet van GenAI bij exclusief aan de overheid toevertrouwde bevoegdheden zoals bijvoorbeeld (maar niet uitsluitend) het nemen van bestuursrechtelijke besluiten of (bijvoorbeeld) de opsporing van misdrijven, hebben wij nu niet onderzocht.

Verder richt dit advies zich op het gebruik van online beschikbare GenAI-toepassingen.

2 Generatieve AI (GenAI)

2.1 Voor het doel van dit advies kan het ontwikkelproces van GenAI, dat op technisch niveau kan worden opgedeeld in vele verschillen fasen[2], worden opgesplitst in twee essentiële verwerkingsfasen: de input- en outputfase.

2.2 Tijdens de inputfase ontvangt het generatieve AI-model een reeks gestructureerde gegevens als input. Deze gegevens kunnen verschillende vormen aannemen, afhankelijk van het type model en de beoogde inzet. Bijvoorbeeld:

> Tekstuele informatie: Als de input tekst is, wordt deze tekst vaak omgezet naar een numerieke representatie. Dit kan worden bereikt door technieken zoals *word embedding* (bijvoorbeeld Word2Vec of GloVe) of door middel van meer geavanceerde benaderingen zoals transformer-gebaseerde modellen, zoals de GPT-architectuur.
>
> Afbeeldingen: In het geval van afbeeldingen worden deze gegevens omgezet in pixelwaarden of representaties in een hoog-dimensionale ruimte, bijvoorbeeld met behulp van convolutionele neurale netwerken (CNN's). Dit stelt het model in staat om complexe visuele patronen te begrijpen.

2.3 Nadat de input correct is verwerkt, en een model is geconstrueerd, onderscheiden wij de outputfase. De outputfase is de operationele fase van het GenAI-model, waarin het model in staat is om output te genereren. Het genereren van output verschilt per type generatieve taak:

> Tekstuele creatie: In dit geval kan het model worden getraind om tekst te genereren op basis van de ontvangen input. Het model zal de context en structuur van de invoer gebruiken om coherente, zinvolle tekst te produceren die past bij de gegeven stijl.
>
> Beeldgeneratie: Voor beeldgeneratie kan een generatief model bijvoorbeeld een decoderend netwerk gebruiken dat op basis van de gegeven input een visuele representatie produceert. Dit kan variëren van het genereren van kunstzinnige afbeeldingen tot het manipuleren van bestaande afbeeldingen.

2.4 Voor de leesbaarheid van dit advies scharen wij *post deployment monitoring* ook onder de outputfase.

[2] De Silva, An artificial intelligence life cycle: From conception to production, Patterns, Volume 3, Issue 6, 2022.

2.5 Post deployment monitoring vindt plaats tijdens de operationele fase van een ontwikkeld GenAI-model, en is bedoeld om fouten, crashes en latenties te detecteren, en ervoor te zorgen dat het model naar behoren blijft functioneren.

2.6 In de rest van dit advies worden de bovenstaande input- en outputfase als leidraad genomen voor de juridische analyse van GenAI.

3 Toepasselijkheid AVG tijdens de inputfase

3.1 Voordat kan worden ingezoomd op de specifieke eisen die de Algemene Verordening Gegevensbescherming (hierna: AVG) stelt aan de ontwikkeling en het gebruik van GenAI tijdens de inputfase, moet eerst worden vastgesteld of de AVG überhaupt van toepassing is. Hiervoor moet worden beschouwd op welke wijze een GenAI-model tot stand komt, en of daarbij persoonsgegevens worden verwerkt.

3.2 Bij de ontwikkeling van GenAI- wordt gebruik gemaakt van verschillende technieken die de modellen in staat stellen om zelfstandig patronen en relaties te vinden in de gegevens, zonder dat hen [expliciet] wordt verteld waarnaar ze moeten zoeken.[3]

3.3 Eenvoudig gezegd worden trainingsgegevens ingevoerd in een statistisch algoritmisch model om als kansverdeling 'brandstof' te fungeren. Door uit de traingingsdata te putten, kan het model op probabilistische wijze inhoud genereren die de trainingsdataset overstijgt.

3.4 Door de band genomen worden GenAI-modellen 'getraind' met miljarden, zo niet honderden miljarden parameters, waarvoor grote hoeveelheden trainingsgegevens en rekenkracht nodig zijn.[4] OpenAI's "CLIP"-beeldclassificator is bijvoorbeeld gebouwd met behulp van een set van 400 miljoen beeld-tekstparen. Het 'BASIC'-model gebruikt zelfs 6,6 miljard van zulke paren.5

3.5 De enorme hoeveelheden gegevens die nodig zijn om GenAI-modellen te trainen brengen mee dat ontwikkelaars van GenAI vaak (moeten) vertrouwen op trainingsgegevens die openlijk beschikbaar zijn op het internet.

> In het geval van ChatGPT wordt het model in de eerste fase (ook wel pre-deployment) getraind op basis van enorme hoeveelheden gegevens die zijn verzameld uit talloze bronnen. Gegevens kunnen afkomstig zijn uit bulkdatabases van externe leveranciers of kunnen worden geëxtraheerd uit enorme hoeveelheden ongestructureerde en ongelabelde gegevens die zijn opgeslagen op het web door middel van scraping- en dataminingtools,

[3] W. Edgar,Chapter 6 - Machine Learning,Editor(s): Thomas W. Edgar, David O. Manz, Research Methods for Cyber Security, Syngress, 2017, p. 153-173.
[4] Ruby, How ChatGPT Works: The Model Behind The Bot, *A brief introduction to the intuition and methodology behind the chat bot you can't stop hearing about*, 2023; https://towardsdatascience.com/how-chatgpt-works-the-models-behind-the-bot-1ce5fca96286
[5] https://openai.com/research/clip

waaronder "persoonlijke informatie die beschikbaar is op het openbare internet".[6] Vervolgens wordt ChatGPT na implementatie opnieuw getraind om zijn prestaties te verbeteren waarbij de input van de gebruiker in dit proces wordt gebruikt.

3.6 Voor het verzamelen van openbaar beschikbare traingingsgegevens wordt veelal gebruik gemaakt van zogenaamde web scraping technieken.

3.7 Web scraping, ook bekend als web harvesting of web data extraction, verwijst naar het geautomatiseerd proces van het extraheren van gegevens van websites. Dit wordt gedaan door een computerprogramma dat webpagina's bezoekt, de HTML-code analyseert en specifieke informatie verzamelt volgens vooraf bepaalde criteria. Deze gegevens kunnen variëren van tekstuele inhoud, zoals artikelen of productbeschrijvingen, tot gestructureerde informatie zoals prijzen, adressen, en meer.

3.8 Het is aannemelijk dat de AVG van toepassing is op de scraping van persoonsgegevens ten behoeve van de ontwikkeling (of het gebruik) van GenAI-toepassingen door medewerlers van de Staat.[7] Door de band genomen is voor de toepasselijkheid van de AVG op het samenstellen van traingingsdata voor GenAI de belangrijkste vraag dus steeds: of met de trainingsdataset persoonsgegevens worden verwerkt?

3.9 Gelet op de omvang van de veelal openbare datasets waarop GenAI-modellen getraind worden, is de kans groot dat daarvan ook persoonsgegevens deel uitmaken. In dit advies nemen wij dan ook tot uitgangspunt dat de AVG van toepassing is op de GenAI tijdens de trainings- ofwel inputfase.

GenAI-modellen persoonsgegevens?

3.10 Opgemerkt moet worden dat in de literatuur discussie bestaat, of de GenAI-modellen *an sich* ook kwalificeren als persoonsgegevens, wanneer de trainginsdataset persoonsgegevens bevat.

3.11 GenAI-systemen zetten trainingsgegevens om in een model dat voorspellingen of classificaties van nieuwe gegevens kan generen op basis van probabilistische patronen die uit die trainingsgegevens zijn gedestilleerd. Hoewel een dergelijk model niet één-op-één de trainingsgegevens bevat, is aangetoond dat met reverse engineering data uit de trainingsdataset kan worden blootgelegd. Dit risico brengt sommige

---

[6] Ruby, How ChatGPT Works: The Model Behind The Bot, *A brief introduction to the intuition and methodology behind the chat bot you can't stop hearing about*, 2023; https://towardsdatascience.com/how-chatgpt-works-the-models-behind-the-bot-1ce5fca96286

[7] Op het scrapen van persoonsgegevens is de AVG van toepassing als dat wordt gedaan in het kader van de activiteiten van een vestiging in de EU van een verwerkingsverantwoordelijke of verwerker, d.w.z. degene die ten behoeve van de ontwikkeling van GenAI de gegevens scraped, ongeacht of de verwerking in de Unie al dan niet plaatsvindt. In aanvulling daarop is de AVG óók van toepassing als er geen sprake is van een vestiging in de unie, maar de gegevens wel worden gebruikt om diensten aan te bieden aan betrokkenen (data subjects) in de unie of om betrokkenen te monitoren. Aldus blijkt uit art 3, lid 1 en 2, AVG.

onderzoekers ertoe te stellen dat de "rechten en verplichtingen inzake gegevensbescherming dan van toepassing zijn op de modellen zelf".[8]

3.12 Andere stellen juist dat deze interpretatie te ver gaat, en onnodige verplichtingen creëert. Deze onderzoekers stellen dat een model geen informatie bevat die redelijkerwijs te relateren valt aan een natuurlijke persoon. Het model, dat gecodificeerde correlaties van numerieke parameters van trainingsgegevens bevat, is eerder het hulpmiddel in dat proces. De noodzakelijke informatie die verwijst naar de natuurlijke persoon is als zodanig niet gecodeerd in het model.[9]

3.13 Om die reden kunnen reverse engineering technieken volgens de betreffende onderzoekers alleen ongestructureerde en anonieme gegevens blootleggen, en niet, zoals bij databases, persoonsgegevens.

3.14 Of een model als zodanig kwalificeert als persoonsgegeven, zal in overwegende mate afhangen van de wijze waarop de trainingsdataset is vormgegeven, en welke beveiliging en anonimiseringsmaatregelen zijn getroffen voor het getrainde model. Dit zal van geval tot geval moeten worden nagegaan, en ligt buiten de scope van dit advies.

3.15 Hieronder wordt de AVG nader toegepast op de verschillende verwerkingen van persoonsgegevens tijdens de inputfase, door achtereenvolgens in te gaan op:

(i) de verwerkingsverantwoordelijkheidsverdeling, (ii) het grondslagvereiste, (iii) het verwerkingsverbod voor bijzondere persoonsgegevens, (iv) het transparantievereiste, (v) dataminimalisatie, en (vi) de rechten van betrokkenen.

4 De inputfase

(i) Verwerkingsverantwoordelijkheidsverdeling (inputfase)

4.1 Voor de beantwoording van de vraag welke partij als verwerkingsverantwoordelijke aangemerkt moet worden is bepalend wie zeggenschap heeft over het doel waarvoor, en de middelen waarmee, de persoonsgegevens worden verwerkt. In artikel 4, onderdeel 7, AVG wordt een verwerkingsverantwoordelijke, voor zover voor dit advies relevant, omschreven als:

> een rechtspersoon of overheidsinstantie die, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

4.2 Het gaat erom of de desbetreffende (rechts)persoon of overheidsinstantie in staat is om zelfstandig te bepalen voor welk doel en met welke middelen de gegevens worden verwerkt. Het kan daarbij betekenis hebben dat deze persoon of instantie daartoe

[8] M R Leiser, Francien Dechesne, Governing machine-learning models: challenging the personal data presumption, International Data Privacy Law, Volume 10, Issue 3, August 2020, p. 193.
[9] Idem.

juridisch bevoegd is, maar dat is geen vereiste. Een (rechts)persoon of overheidsinstantie kan in juridische zin weliswaar onbevoegd zijn met betrekking tot de verwerking van de gegevens, maar niettemin feitelijk wel daarover zeggenschap hebben. En in dat geval kwalificeert deze rechtspersoon of instantie wel als verwerkingsverantwoordelijke. Zowel de zgn. Art. 29 Werkgroep (hierna: WP29) als de opvolger daarvan, de European Data Protection Board (EDPB) typeert de 'verwerkingsverantwoordelijke' dan ook als een functioneel begrip dat beoogt de verantwoordelijkheid daar te leggen waar de feitelijke zeggenschap of invloed met betrekking tot de gegevensverwerkingen ligt.

> Aldus EDPB Richtsnoeren 07/2020 over de begrippen "verwerkings-verantwoordelijke" en "verwerker" in de AVG, versie 2.0, 7 juli 2021; WP29, Advies 1/2010 over de begrippen 'voor de verwerkingsverantwoordelijke' en 'verwerker', (WP169), 16 februari 2010, p. 10; Zwenne, in: *T&C Privacy- en gegevensbeschermingsrecht*, art. 4 AVG, aant. 7.

4.3 De verwerker is, naast de verwerkingsverantwoordelijke, de belangrijkste normadressaat van de AVG. Voor zover voor dit advies relevant wordt de verwerker omschreven als:

> een [..] rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.

4.4 Uit deze begripsomschrijving kan worden opgemaakt dat een verwerker een (rechts)persoon, overheidsinstantie, dienst of orgaan is, die of dat (a) los van de verwerkingsverantwoordelijke staat, en (b) en die of dat persoonsgegevens voor de verwerkingsverantwoordelijke verwerkt, en onder diens verantwoordelijkheid – en dus niet voor zichzelf.

> EDPB Richtsnoeren 07/2020 over de begrippen "verwerkingsverantwoordelijke" en "verwerker" in de AVG, versie 2.0, 7 juli 2021; WP29, 'Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"', 16 februari 2010, p. 28.

4.5 Voor de beoordeling of een organisatie wordt aangemerkt als verwerker zijn de volgende, door WP29 en EDPB ontwikkelde criteria behulpzaam:

- de uitvoerigheid van de opdracht die de verwerkingsverantwoordelijke verstrekt: hoe minder vrijheid, hoe eerder sprake is van een verwerker (en géén verwerkingsverantwoordelijke);
- het toezicht van de verwerkingsverantwoordelijke op de uitvoering van de dienst: hoe frequenter en zorgvuldiger het toezicht, hoe eerder sprake is van een verwerker (géén verwerkingsverantwoordelijke);
- de deskundigheid van de partijen: hoe meer deskundigheid er is bij een organisatie, hoe eerder deze kan worden gekwalificeerd als verwerkingsverantwoordelijkheid (en niet als verwerker);

- de zichtbaarheid of het beeld dat de organisatie bij betrokkenen doet ontstaan en de verwachtingen die betrokkenen hebben op grond van die zichtbaarheid: hoe meer zichtbaar een organisatie is voor betrokkenen, hoe waarschijnlijker het is dat deze wordt aangemerkt als verwerkingsverantwoordelijke (en niet als verwerker).

4.6 Of een organisatie die persoonsgegevens gebruikt om een GenAI-model te trainen als verwerkingsverantwoordelijke of als een verwerker kwalificeert, hangt af van de mate waarin de organisatie het doel bepaalt waarvoor de gegevens worden gebruikt en welke essentiële middelen worden gebruikt voor de verwerking. Het volgende schema bespreekt deze variabelen in de context van het trainen van AI:

Functie	**Activiteiten die wijzen op een verwerkingsverantwoordelijke**	**Activiteiten die wijzen op een verwerker**
Doel van de verwerking		
Waarom de AI wordt getraind.	Als een organisatie zelf besluit om persoonsgegevens te gebruiken om een AI te trainen, is dit een indicatie dat die organisatie verwerkingsverantwoordelijk is.	Als een organisatie persoonsgegevens gebruikt die door een derde partij zijn verstrekt om een AI te trainen, en dit doet op aanwijzing van de derde partij, dan kan de organisatie worden beschouwd als een verwerker.
Essentiële middelen		
Welke persoonsgegevens	Als een organisatie selecteert welke gegevensvelden worden gebruikt om een AI te trainen, is dit een indicatie dat die organisatie verwerkingsverantwoordelijk is.	Als een organisatie van een derde de opdracht krijgt om bepaalde gegevenstypen te gebruiken om een AI te trainen, kan de organisatie een verwerker zijn.
Vaststellen bewaartermijn trainingsdata	Als een organisatie bepaalt hoe lang de AI trainingsgegevens mag bewaren, is dit een indicatie dat die organisatie verwerkingsverantwoordelijk is.	Als een organisatie de opdracht krijgt van een derde partij om gegevens te gebruiken om een AI te trainen en geen controle heeft over hoe lang de AI toegang heeft tot de trainingsgegevens, kan de organisatie een verwerker zijn.
Ontvangers van de persoonsgegevens	Als een organisatie bepaalt welke derden toegang hebben tot de trainingsdata die aan de AI worden verstrekt, is dit een indicatie dat die organisatie verwerkingsverantwoordelijk is.	Als een organisatie van een derde de opdracht krijgt om gegevens te gebruiken om een AI te trainen, maar niet bepaalt wie toegang krijgt tot de AI (en tot de trainingsgegevens waartoe de AI toegang heeft),

		dan is de organisatie mogelijk een verwerker.
Personen van wie de informatie is opgenomen	Als een organisatie selecteert wiens persoonlijke gegevens worden gebruikt als onderdeel van het trainen van een AI, is dit een indicatie dat die organisatie verwerkingsverantwoordelijk is.	Als een organisatie de opdracht krijgt van een derde partij om gegevens van bepaalde personen te gebruiken om een AI te trainen, kan de organisatie een verwerker zijn.

4.7 In paragraaf 5 wordt nader ingegaan op de vraag hoe de Staat in termen van verwerkingsverantwoordelijkheid kwalificeert bij het gebruik van een GenAI-toepassing.

(ii) Het grondslagvereiste tijdens de inputfase

Grondslag ontwikkelen van een (online) GenAI-toepassing

4.8 In het recente handhavingsbevel van Garante tegen OpenAI, richt de fundamentele kritiek van deze toezichthouder zich op het ontbreken van een verwerkingsgrondslag bij de ontwikkeling van ChatGPT.

4.9 Voorafgaand aan het handhavingsbesluit beriep OpenAI zich op artikel 6, eerste, lid, onder b, AVG (uitvoering overeenkomst) om persoonsgegevens te verwerken voor de initiële training (inputfase) van het GPT-model.

4.10 In reactie op het handhavingsbesluit van Garante heeft OpenAI haar verwerkingsgrondslag gewijzigd. Voor de verzameling van gegevens ten behoeve van trainingsdata (inputfase) vertrouwt OpenAI sinds begin april op artikel 6, eerste, lid, onder f, AVG (gerechtvaardigd belang).[10]

4.11 Voorlopig aanvaart Garante deze nieuwe grondslag, mede omdat OpenAI verschillende maatregelen heeft getroffen die het makkelijker voor betrokkenen maken om hun AVG-rechten uit te oefenen. De Italiaanse toezichthouder merkt over de nieuwe grondslag het volgende op:

> Having regard to the information gathered from OpenAI, which stated, inter alia, its willingness to cooperate with the Garante in its letters of 6 and 7 April 2023, and also requested the lifting of the temporary limitation decision;
>
> Finding that it is possible to proceed with re-assessing the circumstances underpinning the temporary limitation decision by making the corresponding determinations, in the light of the information obtained and the willingness

[10] Garante, ChatGPT: OpenAI reinstates service in Italy with enhanced transparency and rights for european users and non-users, 28 april 2023; https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9881490#english

> expressed by the Company to put in place concrete measures to protect the rights and freedoms both of the data subjects whose data have been processed to train the algorithms used to provide the ChatGPT service and of the users of that service, without prejudice to the continuation of the fact-finding activities initiated by the Garante, on condition that OpenAI factually implements the measures specified below which the Company is ordered to take pursuant to Article 58(2)(d) of the Regulation:
>
> (…)
>
> 5. changing the legal basis of the processing of users' personal data for the purpose of algorithmic training, by removing any reference to contract and relying on consent or legitimate interest as legal bases by having regard to the assessment the Company is required to make from an accountability perspective;
>
> 6. making available, on the Company's website, at least to users who are connected from Italy, an easily accessible tool by which to exercise their right to object to the processing of their own data as acquired when using the service for the purpose of training algorithms, where the legal basis chosen under point 5 above is the Company's legitimate interest;
>
> Zie: Garante, ChatGPT: OpenAI reinstates service in Italy with enhanced transparency and rights for european users and non-users, 28 april 2023; https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9881490#english

4.12 Relevant in dit verband is ook de beslissing van de Franse toezichthoudende autoriteit (CNIL) met betrekking tot ClearviewAI's web scraping van gezichtsopnames.[11] Hoewel duidelijk is dat de aard van de persoonsgegevens die door ClearviewAI werden verwerkt verschillen van de gegevens die worden ingevoerd in Large Language Models (LLM's) zoals GPT-4, zijn sommige van de argumenten die CNIL gebruikte in de ClearviewAI-uitspraken mogelijk ook van toepassing op de gegevensverwerking die ten grondslag ligt aan andere GenAI-modellen.

4.13 Relevant is onder meer dat CNIL het volgende overwoog ten aanzien van artikel 6, eerste lid, onder f, AVG:

> 60. As regards the legal basis related to the legitimate interests pursued by the data controller, as provided for in Article 6. 1. (f) of the Regulation, it should be recalled that the "publicly accessible" nature of data does not affect the qualification of personal data and that there is no general authorisation to re-use and further process publicly available personal data, particularly without the knowledge of the data subjects.

[11] CNIL, Facial recognition: 20 million euros penalty against CLEARVIEW AI, 20 oktober 2022; https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai

61. By way of illustration, the Article 29 Working Party (called "WP29" now the EDPB), in its Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, noted in this respect that "personal data, even if it has been made publicly available, continues to be considered as personal data" and that "its processing therefore continues to require appropriate safeguards". While acknowledging that the fact that personal data is publicly available may be a relevant factor in concluding that there are legitimate interests, the EDPB then warned that this would only be the case "if the publication was carried out with a reasonable expectation of further use of the data for certain purposes (e.g. for purposes of research or for purposes related to transparency and accountability)."

62. Furthermore, in order for the data controller to be able to avail itself of these legal grounds, processing must be necessary for the purposes of the legitimate interests it pursues, unless the interests or the fundamental rights and freedoms of the data subjects take precedence.

63. Even if the company's interests were based on the economic interest it derives from the operation of the database in question, this interest should, however, be balanced against the interests or fundamental rights and freedoms of the data subjects, taking into account the reasonable expectations of the individuals based on their relationship with the data controller, in accordance with Article 6.1(f) AVG, read in the light of Recital 47 and the aforementioned opinion on the notion of legitimate interest.[12]

(Onderstreping toegevoegd)

4.14 Uit het bovenstaande volgt dat openbare gegevens niet zonder meer kunnen worden gebruikt voor het samenstellen van trainingsdatasets. Tegelijkertijd zet CNIL de deur open voor het gebruik van artikel 6, eerste lid, onder f, AVG, ter behartiging van de gerechtvaardigde belangen van de ontwikkelaar. Het nastreven van een zuiver economisch belang staat daar, uiteraard, niet aan in de weg.[13]

4.15 Van belang is steeds dat er een juiste balans wordt gevonden tussen de gerechtvaardigde belangen van de ontwikkelaar, en de fundamentele rechten en vrijheden van de betrokkene. Waarbij bijzonder gewicht moet worden gegeven aan de redelijke verwachtingen van de betrokkene.[14]

Conclusie

[12] Idem.
[13] Zie voor een afwijkende opvatting: AP, Normuitleg grondslag 'gerechtvaardigd belang'; https://autoriteitpersoonsgegevens.nl/uploads/imported/normuitleg_gerechtvaardigd_belang.pdf
[14] HvJ EU 4 juli 2023, zaak C-252/21, ECLI:EU:C:2023:537 (Meta vs Bundeskartellamt), nr 109.

4.16 Voor het verwerken van persoonsgegevens in traingingsdata ten behoeve van het ontwikkelen van een openbaar beschikbare (online) GenAI-toepassingen, kan onder voorwaarden een beroep worden gedaan op artikel 6, eerste lid, onder f, AVG.

(iii) Het verwerkingsverbod voor bijzondere persoonsgegevens tijdens de inputfase

4.17 De verwerking van bijzondere persoonsgegevens in de trainingsdata brengt een extra complexiteit met zich, gelet op het verwerkingsverbod uit artikel 9, eerste lid, AVG. Belangrijk hierbij is ook dat het HJEU een brede en contextuele benadering van het concept 'bijzondere persoonsgegevens' hanteert.

4.18 Op 1 augustus 2022 sprak het Hof van Justitie van de Europese Unie (**"HJEU"**) in de zaak C-184/20 (*Etikos*) zich uit over de mate van bescherming van - potentieel - gevoelige gegevens.

4.19 De analyse van het HJEU richt zich op bepaalde gegevens die, hoewel ze niet inherent "bijzonder" zijn, zoals bepaald in artikel 9, eerste lid, AVG, wel het potentieel hebben om gevoelige informatie te onthullen. In dit verband overwoog het HJEU hoe naamsgebonden gegevens met betrekking tot de echtgenoot, samenwonende of partner van de betrokkene het seksleven of de seksuele geaardheid van laatstgenoemde en van zijn partner kunnen onthullen.[15] Het HJEU concludeert dat de mogelijkheid tot het afleiden van bijzondere gegevens door "het leggen van beredeneerde verbanden of door deductie" een voldoende voorwaarde is om het verwerkingsverbod uit artikel 9, eerste lid, AVG, uit te breiden. Helaas gaat het Hof niet verder in op de vraag hoe "het leggen van beredeneerde verbanden of deductie" moet worden uitgelegd.

4.20 Uitgaande van de ruime opvatting van het begrip bijzondere persoonsgegevens, zoals gehanteerd door het HJEU, bestaat een aanzienlijke kans dat trainingsdata verkregen via open bronnen (web scraping), bijzondere persoonsgegevens bevatten. Om die reden wordt hieronder nader ingegaan op de eventuele toepassing van zogenaamde doorbrekingsgronden van het verwerkingsverbod uit artikel 9, eerste lid, Avg.

4.21 Artikel 9, tweede lid, AVG bevat een lijst met uitzonderingen op het algemene verbod om bijzondere persoonsgegevens te verwerken. Voor de ontwikkeling van GenAI-modellen zijn de relevante uitzonderingen die uit artikel 9, tweede lid, AVG de uitdrukkelijke toestemming van betrokkene (onderdeel a), en verwerking met het oog op wetenschappelijk onderzoek of statistische doeleinden (onderdeel j).

Artikel 9, tweede lid, onder a, AVG

4.22 Het algemene verbod op de verwerking van bijzondere persoonsgegevens geldt niet als de betrokkene zijn uitdrukkelijke toestemming geeft voor de betreffende

[15] HvJ EU 1 augustus 2022, zaak C-184/20, ECLI:EU:C:2022:601, (Etikos).

verwerking. Geldige toestemming voor de doorbreking van het verwerkingsverbod vereist dat de toestemming "specifiek" en "geïnformeerd" is, en vereist een "ondubbelzinnige wilsuiting van de betrokkene waarmee deze door middel van een verklaring of een duidelijke bevestigende handeling te kennen geeft in te stemmen met de verwerking van hem betreffende persoonsgegevens."[16]

4.23 Het is niet eenvoudig om aan al deze voorwaarden te voldoen. Zeker wanneer de trainingsdata samengesteld is op basis van web scraping lijkt het verkrijgen van toestemming praktisch onmogelijk. In veel gevallen lijkt toestemming van de betrokkene als doorbrekingsgrond daarom geen reële mogelijkheid voor het verwerken van trainginsdata tijdens de inputfase.[17]

4.24 Echter, het is niet uitgesloten dat GenAI ontwikkelaars kunnen vertrouwen op toestemming als bedoeld in artikel 9, tweede lid, onder a, AVG voor het verwerken van bijzondere persoonsgegevens in trainingsdata. Het gaat dan enkel om die gevallen waarin trainingsdata wordt samengesteld op basis van de input die gebruikers leveren bij het gebruik van reeds werkzame toeppassingen (zie voor de verwerking van bijzondere persoonsgegevens tijdens de outputfase randnr. 5.37), of wanneer op andere wijze gegevens die worden verwerkt als trainingsdata direct van betrokkenen worden verkregen.

4.25 Dat laatste is bijvoorbeeld denkbaar in het geval gewerkt wordt met een kleine dedicated dataset die is samengesteld op basis van een uitvraag aan betrokkenen. Voorbeelden van methoden die op basis van lokale datasets een model ontwikkelen zijn *federated learning* en *transfer learning* (zie daarover nader paragraaf 6).

Artikel 9, tweede lid, onder j, AVG

4.26 Naast uitdrukkelijke toestemming is verwerking van bijzondere persoonsgegevens voor wetenschappelijk onderzoek of voor statistische doeleinden mogelijk op grond van artikel 9 tweede lid, onderdeel j, AVG jo. artikel 24 UAVG, met inachtneming van de volgende voorwaarden:

> a. de verwerking noodzakelijk is met het oog op wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, eerste lid, van de verordening;
>
> b. het onderzoek, bedoeld in onderdeel a, een algemeen belang dient;
>
> c. het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost; en

[16] Artikel 7 AVG.
[17] European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679 (EDPB 2020).

d. bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

4.27 Denkbaar is dat in sommige gevallen de verwerking van trainingsdata voldoet aan bovenstaande vereisten.

4.28 Zo kan het zijn dat zonder de beschikbare trainingsdataset slechts een incomplete, en daarmee ontoereikende dataset beschikbaar is voor het doen van wetenschappelijk onderzoek. Ook is denkbaar dat het onderzoek een duidelijk algemeen belang dient. Daarbij is ook niet ondenkbaar dat uitdrukkelijke toestemming in sommige gevallen onmogelijk zal blijken. Van belang blijft daarbij steeds dat voldoende waarborgen zijn getroffen om dat de persoonlijke levenssfeer van de betrokkene te beschermen.

Conclusie

4.29 Het is niet uitgesloten dat ontwikkelaars van (online) GenAI-toepassingen in specifieke gevallen kunnen vertrouwen op toestemming, zoals bedoeld in artikel 9, tweede lid, AVG, voor het verwerken van bijzondere persoonsgegevens in trainingsdata. Echter, in de meeste gevallen zal het verkrijgen van toestemming praktisch niet haalbaar zijn.

4.30 Ook is het denkbaar dat in specifieke gevallen een beroep kan worden gedaan op artikel 9 tweede lid, onderdeel j, AVG jo. artikel 24 UAVG, als doorbrekingsgrond van het verwerkingsverbod, voor de ontwikkelingen van GenAI-modellen.

(iv) Het transparantievereiste tijdens de inputfase

4.31 De complexiteit van GenAI-verwerkingen en het feit dat een dergelijke verwerking niet volledig kan worden overzien, zelfs niet door de ontwikkelaar, maakt het bijzonder moeilijk om aan het transparantievereiste, zoals bedoeld in artikel 5, eerste lid, onder a, AVG, te voldoen.

4.32 In artikelen 12, 13 en 14 AVG wordt nader uitvoering gegeven aan het transparantievereiste. Uit deze artikelen volgt dat de verstrekte informatie beknopt, transparant, en begrijpelijk moet zijn, almede dat deze een gemakkelijk toegankelijke vorm heeft en in duidelijke en eenvoudige taal is verwoord.[18]

4.33 Om aan deze vereisten te voldoen, moet de aanbieder van GenAI passende maatregelen nemen. Daarmee wordt uitgedrukt dat er sprake moet zijn van een redelijke verhouding tussen, enerzijds, het belang van de betrokkene bij het ontvangen van de informatie in beknopte en voor hem of haar begrijpelijke en

[18] Zie overweging 58; WP29, Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, (WP260rev.01), 29 november 2017 laatst. gew. 11 april 2018, nr. 11.

toegankelijke vorm en, anderzijds, de moeite die de verwerkingsverantwoordelijke daarvoor moet doen.[19]

4.34 De zorgplicht met betrekking tot de beknoptheid, begrijpelijkheid en toegankelijkheid van de informatie geldt 'in het bijzonder' als de informatie specifiek voor een kind is bestemd. Van de verwerkingsverantwoordelijke wordt dus verwacht dat hij ervoor zorg draagt dat de te verstrekken informatie door kinderen gemakkelijk kan worden begrepen (overweging 58 AVG).[20]

4.35 Bij het samenstellen van trainingsdata middels web scraping technieken is in het bijzonder de informatieverplichting uit artikel 14 AVG relevant. Artikel 14 regelt de informatieverstrekking wanneer persoonsgegevens niet bij de betrokkene zelf zijn verkregen. De in dat geval te verstrekken informatie wijkt op onderdelen af van de informatie die op grond van artikel 13 eerste en tweed lid, AVG moet worden verstrekt als de gegevens bij de betrokkene worden verkregen.

4.36 In aanvulling op de, op grond van de bepaling van artikel 13 AVG te verstrekken informatie, moet de betrokkene ook worden geïnformeerd over de categorieën van persoonsgegevens (onderdeel d). Verder moet de betrokkene, evenals bij artikel 13 AVG, de identiteit worden medegedeeld van de verwerkingsverantwoordelijke en de contactgegevens van een functionaris voor gegevensbescherming, alsmede wat de doeleinden zijn waarvoor de gegevens worden verwerkt.

4.37 Ook moet informatie worden verstrekt over de ontvangers van de persoonsgegevens en, als daarvan sprake is, informatie over de doorgifte van de gegevens naar derde landen of internationale organisaties, zijnde: of er al dan niet sprake is van een adequaatheidsbesluit dan wel, wanneer gebruik wordt gemaakt van passende waarborgen, welke dat dan zijn en waar de betrokkene deze kan raadplegen.

4.38 Het is evident zeer ingewikkeld voor ontwikkelaars van GenAI om voor het samenstellen van trainingsdatasets te voldoen aan de bovenstaande informatieverplichtingen.

4.39 Gekeken moet daarom worden of de betreffende ontwikkelaar een beroep toekomt aan artikel 14, vijfde lid, AVG. Op grond van deze bepaling vervalt de verplichting om de betrokkene te informeren wanneer naleving onmogelijk is, onevenredige inspanningen vergt of afbreuk doet aan de verwezenlijking van het doel van de verwerking (artikel 14, lid 5, onder b)):

19 Zie WP29, Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, (WP260rev.01), 29 november 2017 laatst. gew. 11 april 2018, p. 16.

20 Zie WP29, Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679, (WP260rev.01), 29 november 2017 laatst. gew. 11 april 2018, p. 11.

4.40 Volgens overweging 62 van de AVG "moet rekening worden gehouden met het aantal betrokkenen, de ouderdom van de gegevens en de vastgestelde passende waarborgen". Zoals de WP29 benadrukt, is er met name sprake van onevenredige inspanning als de gegevens zijn verzameld van een groot aantal personen van wie ook de contactgegevens onbekend zijn.[21]

4.41 De praktijk wijst uit dat GeAI-aanbieder nog worstelen met het verstrekken van informatie over hun verwerkingspraktijken. Dit geldt ook voor de informatie die wordt verstrekt over het samenstellen van de trainingsdata. In het geval van ChatGPT is het bijvoorbeeld zelfs notoir ondoorgrondelijk waaruit de trainingsdata bestaat. Ook blijkt uit de praktijk niet dat er een actief beroep wordt gedaan op de uitzondering van artikel 14, vijfde lid, AVG.

Conclusie

4.42 Het transparantievereiste is een belangrijke juridische hobbel voor ontwikkelaars van GenAI. Echter, niet is uitgesloten dat aan het transparantievereiste kan worden voldaan, of dat een beroep op een uitzondering mogelijk is. Vooralsnog laat de praktijk niet zien dat op adequate wijze wordt omgegaan met de op de GenAI-ontwikkelaar rustende informatieverplichtingen tijdens de inputfase.

(v) Dataminimalisatie tijdens de inputfase

4.43 Een inherent problematisch vereiste in het kader van GenAI vormt artikel 5, eerste lid, onder c, AVG, waarin staat dat de verwerking van persoonsgegevens "adequaat, ter zake dienend en beperkt moet zijn tot hetgeen noodzakelijk is in verhouding tot de doeleinden waarvoor zij worden verwerkt", oftewel het principe van dataminimalisatie.

4.44 Minimalisatie is gericht op het optimaliseren van de verwerking vanuit het oogpunt van gegevensbescherming, door de gegevensverwerkingsbehoeften in de verschillende fasen te analyseren en waar nodig te beperken. Van belang is dat nagedacht is over de volgende beperkingen van de trainingsdataset:

- Beperking van de omvang van de gegevenscategorieën die worden gebruikt tot de gegevens die strikt noodzakelijk en relevant zijn.
- Beperking van de mate van detail of nauwkeurigheid van de informatie, waarbij ook wordt gelet op de granulariteit van de informatie.
- Beperking van de omvang van het aantal betrokkenen van wie gegevens worden verwerkt.

4.45 Er bestaat een spanning tussen het zogenaamde principe van dataminimalisatie en het idee van big data en data analytics, waarbij statistische methoden worden gebruikt om

[21] WP29, 'Guidelines on Transparency under Regulation 2016/679', 17/EN WP260 rev.01, 11 April 2018, p. 28-31.

nieuwe onverwachte correlaties te ontdekken in enorme datasets. In haar rapport van juni 2020 stelt de Scientific Foresight Unit van het Europees parlement (STOA), dat de voornoemde spanning kan worden wegenomen door dataminimalisering te koppelen aan het idee van evenredigheid. STOA overweegt daarover als volgt:

> (…) the idea of minimisation should be linked to an idea of proportionality. Minimisation does not exclude the inclusion of additional personal data in a processing, as long as the addition of such data provides a benefit, relatively to the purposes of the processing that outweigh the additional risks for the data subjects. Even the utility of future processing may justify retaining the data, as long as adequate security measures are in place. In particular, pseudonymisation, in combination with other security measures, may contribute to limit risks and increase therefore the compatibility of retention with minimisation.[22]

4.46 Uit het voorgaande volgt dat bulkgegevens kunnen worden gebruikt voor zover een dergelijke verwerking, zwaarder weegt dan de risico's die het toevoegt voor de betrokkenen.

4.47 Daarbij spelen ook de verschillende dataminimalisatietechnieken die kunnen worden toegepast een belangrijke rol.

- Voorafgaande analyse van de voorwaarden waaraan de gegevens moeten voldoen om te worden beschouwd als van hoge kwaliteit en met een hoog voorspellend vermogen voor de specifieke toepassing.
- Kritische analyse van de mate van noodzakelijkheid betreffende de soorten gegevens gebruikt in elke fase van de GenIA-oplossing.
- Verwijderen van ongestructureerde gegevens of onnodige informatie die is verzameld tijdens het voorbewerken van informatie. Identificatie en beperking van gegevenscategorieën die geen significante invloed hebben op het leer- of inferentie-resultaat.
- Onderdrukking van irrelevante bevindingen die verband houden met persoonsgegevens tijdens het trainingsproces.
- Gebruik van verificatietechnieken waarvoor minder gegevens nodig zijn, zoals kruisvalidatie.[23]
- Analyse en configuratie van hyperparameters die van invloed kunnen zijn op de hoeveelheid van de verwerkte gegevens.[24]
- Gebruik van federated learning in plaats van gecentraliseerde leermodellen.

---

22 STOA, The impact of the General Data Protection Regulation (GDPR) on artificial intelligencehttps://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

23 Kruisvalidatie houdt in dat de database meerdere keren wordt opgesplitst in trainen en testen, met een verschillende selectie van gegevens in elke subgroep, waarbij het resultaat van het trainen en testen van het algoritme in elke iteratie wordt vergeleken.

24 Hyperparameters zijn parameters waarmee de werking van een specifiek AI-model kan worden geconfigureerd.

- Anonimisering en pseudonimisering, niet alleen bij het rapporteren van gegevens, maar ook bij trainingsgegevens, mogelijke persoonlijke gegevens in het model, en bij het verwerken van inferenties.

Conclusie

4.48 Dataminimalisatie blijft een moeilijk te nemen horde voor de ontwikkeling van GenAI. Veel hangt af van de wijze waarop de trainingsdata tot stand is gekomen. In het geval van de verwerking van bulk gegevens (scraping) zal steeds een duidelijke belangenafweging moeten zijn gemaakt. Van belang blijft steeds dat voldoende waarborgen zijn getroffen om de persoonlijke levenssfeer van de betrokkene te beschermen.

(vi) GenAI en rechten van betrokkenen tijdens de inputfase

4.49 GenAI werpt ook specifieke vragen op met betrekking tot de rechten van betrokkenen uit Hfdst. III AVG. Hieronder worden enkele van die rechten besproken die in het bijzonder worden geraakt door GenAI-toepassingen.

Artikel 16 AVG

4.50 Als persoonsgegevens onjuist of onvolledig zijn, kan de betrokkene van de verwerkingsverantwoordelijke verlangen dat hij de gegevens verbetert of aanvult. Dit moet dan onverwijld (‘without undue delay’) gebeuren (overweging 65).

4.51 De verantwoordelijke voor de verwerking is verplicht om te voldoen aan het recht op rectificatie van de gegevens van de betrokkenen, in het bijzonder de gegevens die zijn gegenereerd door de GenAI-toepassing, maar ook verkeerde trainingsdata zal moeten worden gecorrigeerd.

4.52 Voor veel GenAi-modellen zal artikel 16 AVG een technische uitdaging vormen. Dit omdat, in veel gevallen persoonsgegevens dusdanig verweven zijn met het model, dat het verwijderen van deze gegevens niet altijd mogelijk zal zijn zonder het model aan te tasten. Om dit probleem te ondervangen zal vanaf het begin van de ontwikkeling van het model, in het bijzonder aandacht moeten zijn besteed aan *privacy by design* (artikel 25 AVG).

Artikel 17 AVG

4.53 Voor de toepassing van artikel 17 AVG brengt de werking van GenAI in het bijzonder problemen met zich. Het recht om te worden gewist (of om te worden vergeten) bestaat uit het recht van de betrokkene om "van de voor de verwerking verantwoordelijke zonder onnodige vertraging te verkrijgen dat de hem betreffende persoonsgegevens worden gewist", wanneer de voorwaarden voor rechtmatige

verwerking niet langer aanwezig zijn (deze voorwaarden staan in artikel 17, eerste lid, AVG).

4.54 Het recht van gegevenswissing houdt in dat de voor de verwerking verantwoordelijke proactief moet optreden om ervoor te zorgen dat de gegevens worden gewist wanneer ze niet langer noodzakelijk zijn voor het doel van de verwerking.

4.55 De gegevens die worden verzameld voor de trainingsfase moeten, in overeenstemming met de bepalingen van artikel 11 van de GDPR, en in overeenstemming met het principe van gegevensminimalisatie, worden gezuiverd van alle informatie die niet strikt noodzakelijk is voor de training van het model.

4.56 Wanneer de trainingsfase van het GenAI-model is voltooid, moet de ontwikkelaar de gegevens wissen, tenzij de noodzaak om de gegevens te bewaren voor het verfijnen of evalueren van het systeem gerechtvaardigd is, of de noodzaak en legitimiteit van het bewaren van de gegevens voor andere doeleinden die verenigbaar zijn met de doeleinden waarvoor ze zijn verzameld, gerechtvaardigd is overeenkomstig de voorwaarden uit artikel 6, vierde lid, AVG.

4.57 Daarbij speelt dezelfde problematiek als bij het correctierecht. In het geval onvoldoende aandacht is besteed aan privacy by design, zal het lastig zijn om gegeven te wissen uit het model zonder het model zelf aan te tasten.

Conclusie

4.58 Uitvoering van de rechten van betrokken vormt een blijvende uitdaging voor GenAI-aanbieders. Om te kunnen voldoen aan de eisen uit artikel 15 tot en met 21 AVG, moeten weldoordachte technische en organisatorische maatregelen worden getroffen, en moet privacy by design worden toegepast door de ontwikkelaar.

5 De outputfase

(i) Verwerkingsverantwoordelijkheidsverdeling (outputfase)

5.1 Tijdens de outputfase is het GenAI-model in staat om output te genereren. De gebruiker zal in de meeste gevallen opdrachten moeten geven aan het model, middels zogenaamde ‘prompts’, om tot de gewenste output te komen. Bij het invoeren van prompts kunnen persoonsgegevens worden verwerkt, datzelfde geldt bij de output die een GenAI genereert.

5.2 Omdat post deployment monitoring onderdeel is van de door ons beschreven outputfase moet ook rekening worden gehouden met persoonsgegevens die door de ontwikkelaar worden gebruikt om het GenAI-model te onderhouden, en naar behoren te laten functioneren.

5.3 Om te beginnen zal, het besluit om in het kader van een verwerkingsproces van persoonsgegevens een GenAI-model toe te passen, een belangrijke indicator zijn voor het aanwijzen van de verwerkingsverantwoordelijke. Immers, de keuze om gebruik te maken van een specifieke GenAI-toepassing zegt iets over wie het doel en de middelen bepaalt. Zeker wanneer prompts worden ingevoerd die persoonsgegevens bevatten is de gebruiker voor deze verwerking (de invoer) aan te merken als verwerkingsverantwoordelijke.

5.4 De verwerkingsverantwoordelijkheidsverdeling ligt anders voor zover het betreffende GenAI-model persoonsgegevens genereert als output. Voor het genereren van deze persoonsgegevens is de aanbieder van het GenAI-model in beginsel verwerkingsverantwoordelijk. Wanneer deze gegevens vervolgens worden overgenomen en verwerkt door de gebruiker, zal de verwerkingsverantwoordelijkheid voor die opvolgende verwerking veelal bij de gebruiker liggen.

5.5 Voor zover persoonsgegevens worden verwerkt te behoeve van post deployment monitoring, bepaalt de ontwikkelaar van het GenAI-model het doel en de middelen voor de betreffende verwerking. De ontwikkelaar is dan ook aan te merken als verwerkingsverantwoordelijk voor de verwerking van persoonsgegevens voor post deployment monitoring.

Conclusie

5.6 Wanneer prompts worden ingevoerd die persoonsgegevens bevatten is de gebruiker voor deze verwerking (de invoer) aan te merken als verwerkingsverantwoordelijke.

5.7 Voor het genereren van deze persoonsgegevens is de aanbieder van het GenAI-model in beginsel verwerkingsverantwoordelijk.

5.8 Voor zover persoonsgegevens worden verwerkt te behoeve van post deployment monitoring, bepaalt de ontwikkelaar van het GenAI-model het doel en de middelen voor de betreffende verwerking.

(ii) Grondslagvereiste tijdens de outputfase

Verwerkingsgrondslag ontwikkelaar (output)

5.9 In sommige gevallen kan een GenAI-model ook persoonsgegevens genereren. Los van de problemen rondom de juistheid van deze gegevens, is ook voor deze gegenereerde persoonsgegevens een verwerkingsgrondslag vereist.

5.10 In dit kader kan een parallel worden getrokken met het Google-Spain arrest van het HJEU, waarin het Hof, zij het met een andere bril, het gerechtvaardigd belang van

Google voldoende acht voor het indexeren van persoonsgegevens in haar zoekmachine. Het HJEU overweegt voor zover relevant als volgt:

> 73 As regards legitimation, under Article 7 of Directive 95/46, of processing such as that at issue in the main proceedings carried out by the operator of a search engine, that processing is capable of being covered by the ground in Article 7(f).
>
> 74 This provision permits the processing of personal data where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject — in particular his right to privacy with respect to the processing of personal data — which require protection under Article 1(1) of the directive. Application of Article 7(f) thus necessitates a balancing of the opposing rights and interests concerned, in the context of which account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter (see ASNEF and FECEMD, EU:C:2011:777, paragraphs 38 and 40).
>
> (…)
>
> 80 It must be pointed out at the outset that, as has been found in paragraphs 36 to 38 of the present judgment, processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous (see, to this effect, Joined Cases C 509/09 and C 161/10 eDate Advertising and Others EU:C:2011:685, paragraph 45).
>
> 81 In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator

> of such an engine has in that processing. However, inasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.
>
> Zie: HvJ EU, 13 mei 2014, zaaknr. C-131/12, ECLI:EU:C:2014:317.

5.11 Uit het bovenstaande volgt ons inziens dat het gebruik van de gerechtvaardigd belang grondslag (artikel 6, eerste lid, onder f, AVG) onder voorwaarden mogelijk is voor het genereren van persoonsgegevens. Van belang daarvoor is steeds dat, de gebruiker effectieve middelen heeft om zijn gegevens te controleren en te rectificeren wanneer dat nodig is. Daarbij zal bij GenAI-modellen bijzonder aandacht moeten worden besteed aan de juistheid van de (persoons)gegevens die worden gegenereerd.

Verwerkingsgrondslag voor invoer van persoonsgegevens door medewerkers van de Staat

5.12 Bij het gebruik van GenAI-toepassingen kunnen ook persoonsgegevens als input worden ingevoerd. In dergelijke gevallen moet de gebruiker een grondslag hebben voor de verwerking van de betreffende persoonsgegevens.

5.13 In het kader van het professioneel gebruik van GenAI door medewerkers van de Staat zal per gebruik moeten worden afgewogen of een beroep kan worden gedaan op een verwerkingsgrondslag, zoals bedoeld in artikel 6, eerste lid, AVG. Belangrijk onderscheid daarbij is welke taak wordt uitgevoerd. In het onderstaande wordt een onderscheid gemaakt tussen bedrijfsmatige werkzaamheden en de uitvoering van een publieke taak.

Bedrijfsmatige werkzaamheden

5.14 Bij het invoeren van persoonsgegevens in een (online) GenAI-toepassing, tijdens de uitvoering van dagelijkse werkzaamheden (dat wil zeggen niet bij de uitvoering van een publiekrechtelijke taak), is verdedigbaar dat er sprake is van de behartiging van een gerechtvaardigd belang, zoals bedoeld in artikel 6, eerste lid, onder f, AVG. Of ook

een beroep kan worden gedaan op artikel 6, eerste lid, onder f, AVG als verwerkingsgrond, hangt af van de uitkomst van de zogenaamde driestappentoets.

5.15 Artikel 6, eerste lid, onder f, AVG stelt drie cumulatieve voorwaarden (driestappentoets) waaraan moet zijn voldaan om een verwerking op basis van een gerechtvaardigd belang mogelijk te maken:

> i) behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde,
> ii) noodzaak van de verwerking van de persoonsgegevens voor de behartiging van gerechtvaardigde belangen, en,
> iii) de fundamentele rechten en vrijheden van de bij de gegevensbescherming betrokken persoon prevaleren niet.
>
> Zie ook (HvJ EU 29 juli 2019, ECLI:EU:C:2019:629 (*Fashion ID*) en HvJ EU 4 mei 2017, C-13/16, ECLI:EU:C:2017:336 (*Rīgas satiksme*)), rechtbank Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111, r.o. 14 en ABRvS 27 juli 2022, ECLI:NL:RVS:2022:2173, r.o. 7.1.

5.16 Toegepast op bedrijfsmatige werkzaamheden kan het zijn dat het gerechtvaardigd belang (stap 1) bij het gebruik van de GenAI-toepassing ziet op productiviteits-, of kwaliteitswinst. Verder is ook voorstelbaar dat kan worden betoogd dat het noodzakelijk is om een GenAI-toepassing in te zetten (stap 2). Zo kan de verwerking van persoonsgegevens noodzakelijk zijn om de beoogde productiviteits- of kwaliteitswinst te verwezenlijken, en kan het zijn dat het betreffende doel redelijkerwijs op geen andere wijze, dan met het gebruik van de betreffende GenAI-toepassing, kan worden bereikt.

5.17 Vervolgens moet het gebruik ook de belangenafweging doorstaan tussen de belangen van de verwerkingsverantwoordelijke of derde enerzijds, en de belangen van de betrokkene anderzijds (stap 3). Bij deze belangenafweging moet in het bijzonder rekenschap worden gegeven aan de volgende factoren:

- de redelijke verwachtingen van betrokkenen;
- de uitvoerbaarheid van de rechten van betrokkenen;
- de ernst van de inmenging op de fundamentele rechten van betrokkenen;
- de (aanvullende) waarborgen die de verwerkingsverantwoordelijke heeft getroffen om de ongewenste gevolgen voor de betrokkenen te voorkomen of beperken;

5.18 Gelet op de bovenstaande factoren kan in het algemeen worden gezegd dat meegewogen zal moeten worden dat GenAI-toepassingen in veel gevallen slechts in beperkte mate de uitvoering van de rechten van betrokkene toelaten (zie daarover randnr. 4.49 in samenhang met 4.31). Ook zal steeds moeten worden vastgesteld of

voldoende waarborgen zijn getroffen om ongewenste gevolgen voor de betrokkene te voorkomen of te beperken.

5.19 Verder is steeds van belang wat de redelijke verwachtingen van de burger zijn. Afgevraagd kan worden of de burger verwacht dat medewerkers van de Staat persoonsgegevens van burgers invoeren in een publiek toegankelijke (online) GenAI-toepassing.

5.20 Vooralsnog lijkt het gebruik van GenAI en de technologie daarachter onvoldoende ingeburgerd om een redelijke verwachting van het gebruik daarvan aan te nemen. De historisch snelle adaptatie van bijvoorbeeld ChatGPT is wel een teken dat in de nabije toekomst het gebruik van ervan voldoende zal zijn ingeburgerd. Echter, vooralsnog zal actief moeten worden geïnformeerd over de inzet van GenAI en de verwerking van persoonsgegevens bij de dagelijkse werkzaamheden van ambtenaren.

5.21 Gelet op het voorgaande is niet uitgesloten dat artikel 6, eerste lid, onder f, AVG een grondslag kan vormen voor de verwerking van persoonsgegevens bij het bedrijfsmatig gebruik van GenAI-toepassing door medewerkers van de Staat. Echter, voorwaarde voor een geslaagd beroep op artikel 6, eerste lid, onder f, AVG zal steeds zijn of voldoende mitigerende maatregelen zijn getroffen door de aanbieder van de betreffende GenAI-toepassing, en of de Staat voldoende kan overzien of de ongewenste gevolgen voor de betrokkene in voldoende mate worden voorkomen of beperkt. Daarbij zal de burger ook moeten worden geïnformeerd over het gebruik van GenAI-toepassingen.

5.22 Voor het gebruik van persoonsgegevens die het resultaat zijn van de bewerkingen van een GenAI-model (output), is ook voorstelbaar dat artikel 6, eerste lid, onder f, AVG daarvoor een verwerkingsgrondslag vormt.

5.23 In aanvulling op hetgeen over deze grondslag hierboven al werd besproken geldt voor het gebruik van outputgegevens in het bijzonder dat de juistheid daarvan moet worden geverifieerd. Wil een medewerker van de Staat persoonsgegevens verwerken die het resultaat zijn van GenAI bewerkingen, moeten daarom voldoende technische en organisatorische maatregelen zijn geïmplementeerd die de juistheid van de persoonsgegevens borgen.

5.24 Zonder verificatie maatregelen zowel aan de kant van de GenAI-aanbieder als aan de kant van Staat, kan niet in voldoende mate tegemoet worden gekomen aan de belangen van de betrokkene (stap 3), en kan geen beroep worden gedaan op artikel 6, eerste lid, onder f, AVG.

Publieke taakuitoefening

5.25 Voor het gebruik van GenAI-toepasssing bij het uitvoeren van publieke taken (lees: taken die voortvloeien uit een wettelijke taak), geldt dat slechts in uitzonderlijke gevallen de betreffende wettelijke taak voldoende ruimte zal bieden voor de rechtmatige invoer van persoonsgegevens in een GenAI-toepassing. Van geval tot geval zal moeten worden beoordeeld of de inzet van GenAI op rechtmatige wijze kan plaatsvinden.

5.26 Datzelfde geldt ook voor het verwerking van persoonsgegevens die het resultaat zijn van de bewerking van een GenAI-toepassing (output).

5.27 Verdere bespreking van de inzet van GenAI voor de publieke taakuitoefening valt buiten de reikwijdte van dit advies.

Verwerkingsgrondslag voor verwerkingen door GenAI (post deployment monitoring)

5.28 Het is belangrijk om op te merken dat ontwikkelaars ook persoonsgegevens verzamelen nadat het GenAI-model is ontwikkeld (ook wel *post-deployment monitoring*). Dit om te zorgen voor voortdurende verbetering en verfijning van het systeem.

Artikel 6, eerste lid, onder a, AVG

5.29 Het handhavingsbesluit van Garante en de implementatie van maatregelen door OpenAI leert ons dat ook toestemming een valide en werkbare grondslag kan vormen voor de verwerking van persoonsgegevens die worden ingevoerd door gebruikers tijdens de ouputfase .

Artikel 6, eerste lid, onder b, AVG

5.30 In een recent besluit van de EDPB over WhatsApp benadrukt de EDPB de moeilijkheid van het gebruik van artikel 6, eerste lid, onder b, AVG voor post-deployment monitoring. De EDPB zegt het zo:

> The EDPB recalls that "controllers should make sure to avoid any confusion as to what the applicable legal basis is" and that this is "particularly relevant where the appropriate legal basis is Article 6(1)(b) AVG and a contract regarding online services is entered into by data subjects", because "[d]epending on the circumstances, data subjects may erroneously get the impression that they are giving their consent in line with Article 6(1)(a) AVG when signing a contract or accepting terms of service"176. Article 6(1)(b) AVG requires the existence of a contract, its validity, and the processing being necessary to perform it. These conditions cannot be met where one of the parties(in this case a data subject) is not provided with sufficient information to know that they are signing a contract, the processing of personal data that

> it involves, for which specific purposes and on which legal basis, and how this processing is necessary to perform the services delivered. For the purposes of service improvement and security features, WhatsApp IE has not relied on any other legal basis to process personal data. These transparency requirements are not only an additional and separate obligation, but also an indispensable and constitutive part of the legal basis.[25]

5.31 Uit het voorgaande volgt ons inziens dat artikel 6, eerste lid, onder b, AVG een bruikbare grondslag kan vormen voor de verwerking van persoonsgegevens ten behoeve van post deployment monitoring, mits de gebruiker op juiste wijze wordt geïnformeerd.

Conclusie

5.32 Voor de verwerking van persoonsgegevens door het GenAI-model kan een geslaagd beroep worden gedaan op verschillende verwerkingsgrondslagen. Het gebruik van de gerechtvaardigd belang grondslag (artikel 6, eerste lid, onder f, AVG) is onder voorwaarden mogelijk voor het genereren van persoonsgegevens.

5.33 Voor post deployment monitoring kan, onder voorwaarden, een geslaagd beroep worden gedaan op artikel 6, eerste lid, onder b, Avg. Daarbij vormt ook toestemming (artikel 6, eerste lid, onder a, AVG) een bruikbare grondslag.

5.34 Gelet op het voorgaande is niet uitgesloten dat artikel 6, eerste lid, onder f, AVG een grondslag kan vormen voor de verwerking van persoonsgegevens bij het bedrijfsmatig gebruik van GenAI-toepassing door medewerkers van de Staat. Echter, voorwaarde voor een geslaagd beroep op artikel 6, eerste lid, onder f, AVG zal steeds zijn of voldoende mitigerende maatregelen zijn getroffen door de aanbieder van de betreffende GenAI-toepassing, en of de Staat voldoende kan overzien of de ongewenste gevolgen voor de betrokkene in voldoende mate worden voorkomen of beperkt. Daarbij zal de burger ook moeten worden geïnformeerd over het gebruik van GenAI-toepassingen.

5.35 Voor het gebruik van persoonsgegevens die het resultaat zijn van de bewerkingen van een GenAI-model (output), is ook voorstelbaar dat artikel 6, eerste lid, onder f, AVG daarvoor een verwerkingsgrondslag vormt.

5.36 Zonder verificatie maatregelen zowel aan de kant van de GenAI-aanbieder als aan de kant van Staat, kan niet in voldoende mate tegemoet worden gekomen aan de belangen van de betrokkene, en kan geen beroep worden gedaan op artikel 6, eerste lid, onder f, AVG.

---

[25] ÉDPB, Binding Decision 5/2022 on the dispute submitted by the Irish SA regarding WhatsApp Ireland Limited (Art. 65 GDPR), nr. 117: https://edpb.europa.eu/system/files/2023-01/edpb_bindingdecision_202205_ie_sa_whatsapp_en.pdf

(iii) Het verwerkingsverbod voor bijzondere persoonsgegevens tijdens de outputfase

5.37 Evenals de verwerking van bijzondere persoonsgegevens tijdens de outputfase geldt voor de verwerking van bijzondere persoonsgegevens dat daarvoor een beroep moet kunnen worden gedaan op een doorbrekingsgrond uit artikel 9, tweede lid, AVG.

5.38 Voor de verwerking van bijzondere persoonsgegevens door de ontwikkelaar tijdens de outputfase wordt verwezen naar de bespreking van de doorbrekingsgronden uitdrukkelijke toestemming van betrokkene (onderdeel a), en verwerking met het oog op wetenschappelijk onderzoek of statistische doeleinden (onderdeel j), zoals hierboven reeds besproken.

5.39 Voor wat betreft de verwerking van bijzondere persoonsgegevens aan de hand van prompts ingevoerd door medewerkers van de Staat, of de verdere verwerking van bijzondere persoonsgegevens die het resultaat zijn van output, geldt dat artikel 9, eerste lid, AVG in een moeilijk te nemen drempel vormt. In de meeste gevallen zal geen beroep kunnen worden gedaan op een doorbrekingsgrond, uit artikel 9, tweede lid, AVG, voor de verwerking van bijzondere persoonsgegevens aan de hand van online beschikbare GenAI-toepassingen.

(iv) Het juistheidsvereiste tijdens de outputfase

5.40 Het beginsel van juistheid volgt uit artikel 5, eerste lid, onder d, AVG. In dat artikel is bepaald dat gegevens nauwkeurig moeten zijn en, indien nodig, worden bijgewerkt worden.

5.41 Omdat GenAI-modellen informatie kunnen generen dat verder strekt dan de trainingsdata waarop zij zijn gemodelleerd, kan het voorkomen dat fouten ontstaan bij de extrapolatie van die gegevens. Wanneer GenAI-modellen vreemde uitkomsten genereren die losstaan van de objectieve werkelijkheid wordt dit ook wel aangeduid als hallucineren.

5.42 Zogenaamde AI-hallucinaties vormen een bedreiging voor de juistheid van eventuele persoonsgegevens die worden gegenereerd door een GenAI-model. In het geval van hallucinaties bestaat met name het risico dat gevoelige persoonsgegevens of bedrijfsgeheimen ten onrechte worden gegenereerd. Daarnaast kunnen objectief valse gegevens leiden tot incidenten op het gebied van gegevensbescherming en/of worden misbruikt door aanvallers.

5.43 Ook het risico van vooringenomenheid, ook wel *bias-risk*, is een risico dat samenhangt met het juistheidvereiste.

5.44 Met betrekking tot de juistheid van de gegevens die over de betrokkene worden verwerkt of afgeleid, zijn er drie factoren die de nauwkeurigheid van de gegevens kunnen beïnvloeden:

- De trainings- of validatiedataset bevat fouten. Deze fouten kunnen optreden wanneer slechte gegevenskwaliteit, ontbrekende gegevens of selectieve steekproeftrekking onderdeel vormen van de trainingsdataset. Deze fouten kunnen ook optreden door de manier waarop de gegevens zijn geformatteerd.
- Er zijn modellen, waarbij het systeem zelf fouten kan introduceren die leiden tot foutieve gevolgtrekkingen. Aan de andere kant is er de mogelijkheid van programmeer- of ontwerpfouten die het model verkeerd vertaalt naar de praktische uitvoering.
- In het geval GenAI wordt ontwikkeld op basis van een beperkte dataset die specifieke kenmerken van een groep uitvergroten en een feedbackloop introduceren.

5.45 Om de juistheid van een GenAI-model te waarborgen moeten meet-, opschonings- en traceerbaarheidstechnieken worden toegepast om de nauwkeurigheid en integriteit van de dataset te garanderen.

Conclusie

5.46 In de outputfase vormt het juistheidsvereiste een uitdaging waarvoor op voorhand mitigerende maatregelen moeten zijn geïmplementeerd door de GenAI-aanbieder.

(v) Transparantievereiste tijdens de outputfase

5.47 Wanneer persoonsgegevens worden verzameld, moet de verwerkingsverantwoordelijke voldoen aan het transparantievereiste uit artikel 12, 13, 14 AVG. De moeilijkheid om te voldoen aan dit vereiste tijden de inputfase werd hierboven al besproken. De gegevens die moeten worden verstrekt tijdens de outputfase zijn niet anders, en omvatten in ieder geval:

- De identiteit van de verwerkingsverantwoordelijke.
- Hoe de verwerkingsverantwoordelijke kan worden gecontacteerd.
- Het doel van de verwerking.
- De rechtsgrondslag voor de verwerking.
- De categorieën van persoonsgegevens die worden verwerkt.

5.48 Er moet ook informatie worden verstrekt over risico's, getroffen maatregelen, en hoe de rechten van betrokkenen kunnen worden uitgeoefend.

5.49 In het geval de Staat gebruik maakt van een GenAI-toepassing zal op de Staat, voor zover zij als verwerkingsverantwoordelijke kwalificeert, de informatieplicht.

Wanneer persoonsgegevens worden verzameld en verder worden verwerkt voor geautomatiseerde besluitvorming geldt een aanvullende informatieplicht. Geautomatiseerde besluiten worden gedefinieerd en geregeld in artikel 22 AVG. Wanneer geautomatiseerde besluiten worden toegepast, moeten maatregelen worden geïmplementeerd om de rechten, vrijheden en rechtmatige belangen van de betrokkene te beschermen. De betrokkene moet kunnen eisen dat een mens de uiteindelijke beslissing neemt en moet het recht hebben om in beroep te gaan. Geautomatiseerde beslissingen die betrekking hebben op speciale categorieën van persoonsgegevens (gevoelige persoonsgegevens) zijn alleen toegestaan als de betrokkene toestemming heeft gegeven of als dit wettelijk is gerechtvaardigd.

6 Methoden voor een betere gegevensbescherming

6.1 GenAI is een technologie die zich snel ontwikkelt. Dat geldt ook voor de tools en methoden die kunnen helpen om de uitdagingen op te lossen die het gebruik van GenAI op het gebied van gegevensbescherming met zich brengt. Hieronder bespreken wij enkele belangrijke technische mitigerende maatregelen.

Generative Adversarial Networks

6.2 Een mogelijke mitigerende maatregel voor het (onbedoeld) verwerken van (bijzondere) persoonsgegevens is het gebruik van een zogenaamd Generative adversarial network (GAN) methoden. Het gebruik van een GAN vermindert de behoefte aan extern verkregen trainingsdata door uitputgegevens te gebruiken om trainingsdata te genereren. Met andere woorden, de output wordt gebruikt om te bepalen hoe de input eruit zal zien, of vice versa.

6.3 Deze methode gebruikt twee neurale netwerken een "generator" en een "discriminator". De generator leert hoe hij gegevens moet samenvoegen om bijvoorbeeld een afbeelding of tekst te genereren die lijkt op de uitput, terwijl de discriminator leert hoe hij het verschil kan zien tussen de echte gegevens en de synthetisch gegenereerde gegevens.

Federated learning

6.4 Federated learning werkt door de laatste versie van een reeds ontwikkeld model. te verbeteren op het apparaat of de servers van de gebruiker, en op basis van lokale gegevens. De wijzigingen aan het model worden daarna teruggekoppeld naar de oorspronkelijke server waar ze worden geconsolideerd met de wijzigingsinformatie van andere modellen. Een gemiddelde van de gewijzigde informatie wordt dan gebruikt om het oorspronkelijke model te verbeteren. Het nieuwe, verbeterde gecentraliseerde model vervolgens weer worden gedownload. Deze methode biedt de mogelijkheid om

een bestaand model te verbeteren op basis van een groot aantal gebruikers, zonder dat de gegevens van de gebruikers gedeeld hoeven te worden.

Transfer learning

6.5 Het is niet altijd nodig om modellen vanaf nul te ontwikkelen. Een andere mogelijkheid is om gebruik te maken van bestaande modellen die vergelijkbare taken oplossen. Door de verwerking te baseren op reeds bestaande modellen, is het vaak mogelijk om hetzelfde resultaat te bereiken met minder gegevens.

7 Generatieve AI-tools en auteursrecht

7.1 Het gebruik van generatieve AI-tools roept, naast privacyrechtelijke vragen, ook verschillende auteursrechtelijke vragen op. Daarbij kan onderscheid worden gemaakt tussen (i) de fase waarin een generatieve AI-tool wordt getraind aan de hand van openbaar verkregen data (de 'input-fase'), en (ii) de fase waarin een generatieve AI-tool al functioneel is en op verzoek output genereert voor eindgebruikers (de 'output-fase'). De belangrijkste auteursrechtelijke risico's (voor de eindgebruiker) die in beide fases spelen, worden hierna afzonderlijk besproken.

Ad (i): de input-fase

7.2 In de input-fase worden generatieve AI-tools veelal getraind aan de hand van een omvangrijke hoeveelheid data. Verondersteld wordt dat deze (bestaande) data doorgaans door middel van scraping van internet (of uit andere bronnen, zoals digitale bibliotheken) is overgenomen. Op basis van de data wordt het AI-model vervolgens getraind om, op een later moment, de door de eindgebruiker gewenste uitkomsten te kunnen genereren.

7.3 Wanneer grote hoeveelheden informatie gescrapetet worden van internet, is het zeer aannemelijk (of: nagenoeg zeker) dat zich onder de gescrapete inhoud (ook) veel auteursrechtelijk beschermde werken bevinden, zoals bijvoorbeeld e-books en foto's.[26] De vraag is of dat auteursrechtelijk gezien is toegestaan. De gebruikte auteursrechtelijke werken kunnen soms bijvoorbeeld uit illegale bron verkregen zijn, en ook los daarvan zijn rechthebbenden veelal niet op de hoogte van het feit dat hun auteursrechtelijke werken voor de ontwikkeling van een generatieve AI-tool gebruikt zijn. Deze rechthebbenden weten het evenmin wanneer hun werken uiteindelijk in de outputfase ten grondslag worden gelegd aan de uiteindelijke output die de AI-tools op verzoek van een eindgebruiker genereren (en zij kunnen dan dus ook niet makkelijk nagaan of die output wel of niet voldoende afstand houdt van hun originele werk).

[26] Uiteraard is ook andere informatie waarop intellectuele-eigendomsrechten rusten denkbaar, zoals databankrechten.

Een, vanuit juridisch oogpunt, extra bemoeilijkende factor daarbij is bovendien dat dit alles plaatsvindt in een internationale context. Auteursrechtelijke werken die te vinden zijn op een Nederlandstalige website kunnen bijvoorbeeld door een Amerikaanse ontwikkelaar van een AI-tool worden gescrapet, waarna die AI-tool vervolgens door personen uit de hele wereld gebruikt wordt, en gegenereerde content vervolgens ook weer over de hele wereld openbaar gemaakt kan worden. Dat alles maakt dat (in theorie) verschillende auteursrechtelijke regimes van toepassing kunnen zijn met onderling verschillende juridische maatstaven voor het vaststellen van een inbreuk of het aannemen van bescherming. In het kader van dit advies hebben wij omwille van de eenvoud zoveel als mogelijk het Nederlandse (en grotendeels Europees geharmoniseerde) auteursrecht centraal gesteld. Dat neemt echter niet weg dat in de praktijk (in individuele gevallen) ook met die buitenlandse juridische regimes rekening gehouden moet worden.

7.4 Onder auteursrechtjuristen wordt aangenomen dat het gebruik van auteursrechtelijke beschermde werken ter training van een AI-model (waarschijnlijk) een verveelvoudigingshandeling is die de rechthebbende kan verbieden.[27] Dat betekent dat ontwikkelaars van generatieve AI-tools het gebruik van auteursrechtelijk beschermd materiaal in de inputfase steeds zullen moeten kunnen legitimeren op grond van (a) toestemming van de rechthebbende(n) of (b) een in de wet neergelegde exceptie op het auteursrechtelijke verveelvoudigingsrecht.

7.5 Mede gelet op de enorme hoeveelheden data die bij de ontwikkeling van (veel) generatieve AI-modellen kunnen worden gebruikt, en de lage drempel die geldt voor het ontstaan van auteursrechtelijke bescherming, waardoor veel creatieve teksten al snel onder het auteursrechtelijke beschermingsregime vallen, is de kans niet groot dat aanbieders van AI-tools steeds van alle relevante rechthebbenden toestemming zullen hebben verkregen. Daarmee resteert een eventueel beroep op een auteursrechtelijke exceptie.

7.6 Alhoewel de toelaatbaarheid van het scrapen van auteursrechtelijk werken in de praktijk als gezegd in concrete gevallen (waarschijnlijk) mede naar maatstaven van buitenlandse auteurswetten beoordeeld dient te worden, zijn binnen de Europese Unie in dat verband vooral de zogeheten auteursrechtelijke 'tekst- en data-mining excepties' van belang.[28] Deze excepties, oorspronkelijk afkomstig uit de artikelen 3 en 4 van de DSM-richtlijn (EU 2019/790), zijn in Nederland geïmplementeerd in de artikelen 15n en artikel 15o Auteurswet:

> Artikel 15n lid 1 Auteurswet:
> "Als inbreuk op het auteursrecht op een werk van letterkunde, wetenschap of kunst wordt niet beschouwd de reproductie door onderzoeksorganisaties en

[27] Maar zie anders: Senftleben, M. Compliance of National TDM Rules with International Copyright Law: An Overrated Nonissue?. IIC 53, 1477–1505 (2022).
[28] Ter vergelijking: binnen de Verenigde Staten zal veelal een beroep moeten worden gedaan op 'fair-use'.

> cultureel erfgoedinstellingen om met het oog op wetenschappelijk onderzoek tekst- en datamining te verrichten op het werk waartoe zij rechtmatige toegang hebben."
>
> Artikel 15o lid 1 Auteurswet:
> "Onverminderd het bepaalde in artikel 15n wordt een reproductie in het kader van tekst- en datamining niet als inbreuk op het auteursrecht op een werk van letterkunde, wetenschap of kunst beschouwd mits degene die de tekst- en datamining verricht rechtmatig toegang heeft tot het werk en het auteursrecht door de maker of zijn rechtverkrijgenden niet uitdrukkelijk op passende wijze is voorbehouden, zoals door middel van machinaal leesbare middelen bij een online ter beschikking gesteld werk." – Onderstreping toegevoegd

7.7 Artikel 15n Auteurswet beperkt zich tot gebruik door onderzoeksorganisaties en cultureel erfgoedinstellingen met het oog op wetenschappelijk onderzoek. In de praktijk zullen commerciële aanbieders van AI-tools zich, voor zover in het kader van scraping een verveelvoudigingshandeling plaatsvindt, veelal (dienen te) beroepen op artikel 15o Auteurswet. Dat betekent echter dat bij de ontwikkeling van een AI-tool geen gebruik mag worden gemaakt van inhoud waartoe op onrechtmatige wijze toegang werd verkregen (zoals bijvoorbeeld door het omzeilen van paywalls), en daarnaast dat er geen gebruik mag worden gemaakt van beschermde inhoud waarvan de rechthebbenden het auteursrecht hebben voorbehouden (een zogenaamde 'opt-out').

7.8 Het valt voor een eindgebruikers en rechthebbenden op dit moment 'vanaf de buitenkant bezien' niet goed na te gaan of ontwikkelaars van AI-tools in de inputfase voldoende met dergelijke auteursrecht-voorbehouden of opt-outs rekening hebben gehouden, en evenmin van welke auteursrechtelijke werken er bij de ontwikkeling van de AI-tool precies wel of niet gebruik is gemaakt. Het feit dat er – in het buitenland - door (vermeend) rechthebbenden het afgelopen jaar verschillende rechtszaken tegen aanbieders van generatieve AI-tools aanhangig zijn gemaakt, doet echter vermoeden dat het rechtenbeheer (minst genomen) lang niet in alle gevallen op orde is:

> Vgl. bijvoorbeeld over een zaak die aanhangig is gemaakt in het Verenigd Koninkrijk tegen Stable Diffusion:
> The Verge: "Getty Images is suing the creators of AI art tool Stable Diffusion for scraping its content", 17 januari 2023[29]
>
> En in de Verenigd Staten tegen Microsoft, GitHub en OpenAI:
> The Verge: "The lawsuit that could rewrite the rules of AI copyright", 8 november 2022[30]

[29] https://www.theverge.com/2023/1/17/23558516/ai-art-copyright-stable-diffusion-getty-images-lawsuit
[30] https://www.theverge.com/2022/11/8/23446821/microsoft-openai-github-copilot-class-action-lawsuit-ai-copyright-violation-training-data

7.9 In lijn hiermee vragen belanghebbenden uit de creatieve industrie daarnaast ook op Europees niveau aandacht voor hun standpunt dat het trainen van AI-modellen op basis van bestaand auteursrechtelijk beschermd materiaal op grote schaal tot auteursrechtinbreuk leidt, en dat dit wetgevend handelen vereist. Vgl. bijvoorbeeld EGAIR.eu:

> "Who is EGAIR and what does it do?
> It is a European alliance founded by creatives, professionals and associations from all over the artistic fields to represent them unitedly in their relations with European institutions and the Media on the issue of the regulation of AI applications in the creative arts.
> What do you think about the use of AI in the creative industries? What are your positions on the issue?
> We believe that major software and AI companies are carrying out an illegitimate exploitation of data for the training of Ai TTI (Text to Image). It is a process that violates both privacy rights and copyrights at different levels on global scale. We believe that the data used in the AI training can be only exploited with the prior consent of the rightful owners or transferred under conditions in accordance with a proper license of use in the case of copyrighted data." - https://www.egair.eu/

7.10 De Europese Commissie heeft het risico op inbreuk op auteursrechten (en andere intellectuele-eigendomsrechten) door aanbieders van AI-tools daarnaast eveneens erkend. In het kader van de naderende Europese AI-Act wordt daarom op dit moment gesproken over de (mogelijke) introductie van een transparantieverplichting die inhoudt dat aanbieders van generatieve AI-tools kenbaar moeten maken welke auteursrechtelijk beschermde werken zij aan hun generatieve AI-tools ten grondslag hebben gelegd.

> Zoals verwoord in het meest recente voorstel van het Europees Parlement dat op dit moment beschikbaar is (maar nog niet definitief is vastgesteld) komt deze transparantieverplichting als volgt te luiden:
>
> "4. Providers of foundation models used in AI systems specifically intended to generate, with varying levels of autonomy, content such as complex text, images, audio, or video ("generative AI") and providers who specialise a foundation model into a generative AI system, shall in addition
> (…)
> without prejudice to national or Union legislation on copyright, document and make publicly available a sufficiently detailed summary of the use of training data protected under copyright law."[31]

[31] https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

7.11 In afwachting van dergelijke regelgeving geldt echter nu nog met onvoldoende zekerheid valt vast te stellen of bij de ontwikkeling van een generatieve AI-tool voldoende rekening is gehouden met auteursrechten van derden. Daarbij komt dat – zoals hiervoor aangegeven – in gevallen waarin (ook) andere jurisdicties van toepasselijk zijn, (mede) naar de maatstaven van de in die jurisdicties geldende auteurswetten bepaald moet worden of sprake is van een inbreuk.

7.12 Het voorgaande leidt samenvattend tot de conclusie dat er een realistische kans bestaat dat bij de ontwikkeling van generatieve AI-tools auteursrechtinbreuken plaatsvinden.

7.13 Dat impliceert nog niet (automatisch) dat ook de eindgebruiker dus, vanwege het mogelijke plaatsvinden van (onrechtmatige) scraping in de inputfase, onrechtmatig handelt als hij of zij in de outputfase van een AI-tool gebruik maakt. Tegelijkertijd bestaat dat risico, in ieder geval in theorie, wel degelijk.

7.14 Zoals volgt uit de hiervoor genoemde rechtszaken, wordt de discussie over de rechtmatigheid van scraping bij het trainen van generatieve AI-tools op dit moment vooral gevoerd tussen auteursrechthebbenden en ontwikkelaars/aanbieders van deze generatieve AI-tools zelf. Dat is echter geen garantie dat deze discussie zich in de toekomst kan verleggen, en dat rechthebbenden op een later moment alsnog zullen besluiten dat ook (grootschalige) eindgebruikers verantwoordelijk moeten worden gehouden, bijvoorbeeld gebaseerd op de stelling dat zij meeliften op het product van (wat de auteursrechthebbenden zien als) een grootschalige auteursrechtinbreuk. De rechtspositie van die eindgebruikers is een dergelijk geval – bij de huidige stand van zaken - relatief ongunstig, omdat (veel) aanbieders van generatieve AI-tools aansprakelijkheid voor inbreuken op intellectuele-eigendom via hun algemene voorwaarden zoveel als mogelijk uitsluiten, en dus goeddeels doorleggen aan de eindgebruikers zelf.

Deze eindgebruikers worden op grond van diezelfde algemene voorwaarden bovendien geen contractueel afdwingbare rechten geboden om zelfstandig na te gaan welke auteursrechtelijke werken aan de ontwikkeling van de AI-tool ten grondslag hebben gelegen. Dat maakt het voor hen daarom lastig zich in het geval van een aansprakelijkstelling te verweren, en feitelijk onmogelijk om op voorhand een volledig en gefundeerd oordeel te vormen over de rechtmatigheid van eventueel gebruik en de auteursrechtelijke risico's daarvan.

Ad (ii): de output-fase

7.15 Als een generatieve AI-tool eenmaal voldoende getraind is en aan eindgebruikers ter beschikking wordt gesteld, dienen zich een aantal andere auteursrechtelijk vragen aan, zoals: (i) de vraag of de door AI voor een eindgebruiker gegenereerde output zelfstandig auteursrechtelijk bescherming geniet, (ii) de vraag bij wie die eventuele auteursrechten dan rusten en (iii) de vraag of de output naar maatstaven van het

auteursrecht (of een ander toepasselijk intellectueel-eigendomsrecht) wel voldoende afstand houdt van eerdere werken, zoals bijvoorbeeld de werken die in de inputfase gebruikt zijn om de generatieve AI-tool te trainen. In het kader van dit advies is voornamelijk laatstgenoemde vraag (iii) van belang.

7.16 Het antwoord op die vraag (iii), valt in individuele gevallen echter (praktisch) niet te geven. De oorzaak daarvan is, ook hier weer, gelegen in het feit dat bij gebrek aan een transparantieverplichting, voor een eindgebruiker in een concreet geval nagenoeg simpelweg niet valt te achterhalen:

- welke oorspronkelijke auteursrechtelijke werken ooit aan de training van een generatieve AI-tool ten grondslag hebben gelegen,
- of de rechthebbende op die werken ooit toestemming hebben verleend hun werk ten behoeve van de betreffende AI-tool te gebruiken en/of gebruik hebben gemaakt van een opt-out in de zin van artikel 15o Auteurswet, en:
- of de uiteindelijk gegenereerde output naar auteursrechtelijke maatstaven (of in andere gevallen: naar maatstaven van andere intellectuele-eigendomsrechten, zoals databankenrechten, merkrechten of modelrechten) voldoende afstand houdt van (onder andere) de originele werken die ooit aan de training van de generatieve AI-tool ten grondslag hebben gelegen. Is dat niet het geval, dan kan bij veel vormen van gebruik van de output immers sprake zijn van een inbreuk op intellectuele eigendomsrechten.

7.17 Eindgebruikers kunnen er op dit moment dus niet op vertrouwen, en ook niet (eenvoudig) nagaan, of datgene wat zij door middel van een AI-tool laten genereren, inbreuk maakt op rechten van derden. Wat de omvang van de kans is dat zij vanwege het gebruik van gegenereerde output aansprakelijk worden gesteld, is in het verlengde daarvan evenmin vast te stellen.

7.18 Op dit moment zijn ons (nog) geen gevallen of rechtszaken bekend waarin eindgebruikers (of hun werkgevers) aansprakelijk werden gesteld voor een inbreuk op het intellectuele-eigendomsrecht vanwege het gebruik van op basis van AI gegenereerde inhoud. Feit is echter wel dat een dergelijke aansprakelijkstelling in voorkomende gevallen dus mogelijk zullen zijn, te meer nu de aanbieders van generatieve AI-tools in hun algemene voorwaarden het risico voor aansprakelijkheid (waaronder vanwege inbreuken op intellectuele eigendom) volledig of grotendeels uitsluiten, of zelfs verlangen dat gebruikers hen vrijwaren voor de gevolgen van eventuele aansprakelijkstellingen:

Vgl. bijvoorbeeld:

- Artikel 3 (a) van de Terms of Use van OpenAI: "[…] You are responsible for Content, including for ensuring that it does not violate any applicable law or these Terms […]"

- Artikel 7 (a) van de Terms of Use van OpenAI: "You will defend, indemnify, and hold harmless us, our affiliates, and our personnel, from and against any claims, losses, and expenses (including attorneys' fees) arising from or relating to your use of the Services, including your Content, products or services you develop or offer in connection with the Services, and your breach of these Terms or violation of applicable law."

- De Bing Chat Enterprise Supplemental Terms van Microsoft:
  "**Ownership of Output**. Microsoft does not claim ownership of the Output Content of the Azure OpenAI Service or BCE. You will need to make your own determination regarding the intellectual property rights you have in Output Content and its commercial usability, taking into account, among other things, your usage scenario(s) and the laws of the relevant jurisdiction. Microsoft reserves all rights in its intellectual property.
  Third-party claims. You are responsible for responding to any third-party claims regarding your use of BCE in compliance with applicable laws (including, but not limited to, copyright infringement or other claims relating to Output Content output during your use of BCE). "

- Zie voor een recente analyse van de gebruiksvoorwaarden van verschillende AI-tools en de scheve verdeling van aansprakelijkheid daarin bijvoorbeeld ook: N. Helberger, Generative AI in Media & Journalism: Think Big, But Read the Small Print First', d.d. 18 juli 2023:

  "An initial review of the Terms of Use of the five providers of generative AI reveals that the contractual reality is far away from this ideal of mutual assistance. Typically, the Terms of Use determine that downstream users bear full responsibility for making sure their use of the technology complies with legal requirements from e.g. data protection and copyright law or the AI Act and is otherwise responsible. All of the Terms of Use examined contain the extensive disclaimers of responsibility typically known from other software contracts. In addition, all include indemnification clauses obliging the downstream user to defend the provider against any claims that may arise from their use of the model, typically at their own costs. None of the terms analysed addressed the situation that safe use of the model or compliance with the applicable laws by downstream users is not possible without the cooperation of the developers of the models themselves. None of the Terms of Use examined included any language of assistance, described a responsibility on the side of the providers of the models to cooperate or any rights to transparency on the side of downstream users."[32]

[32] https://generative-ai-newsroom.com/generative-ai-in-media-journalism-think-big-but-read-the-small-print-first-375f2ecb1256

Niet-auteursrechtelijke contractuele beperkingen op gebruik output

7.19 Uit de algemene voorwaarden en gebruiksrichtlijnen van aanbieders van generatieve AI-tools volgens overigens soms ook (niet-auteursrechtelijke) beperkingen op het gebruik van gegeneerde content. Zo bepaalt de Sharing & publication policy (november 2022) van ChatGPT (OpenAI) bijvoorbeeld dat content die mede op basis van ChatGPT tot stand is gekomen, alleen op sociale media gedeeld mag worden onder duidelijke vermelding van het feit dat de content deels op basis van AI gegeneerd is. Ook mag de betreffende inhoud (of het onderwerp daarvan) geen inbreuk maken op de content policy en de terms of use van OpenAI.[33]

7.20 Gebruik van ChatGPT voor politieke campagnedoeleinden is daarnaast in het geheel niet toegestaan. Dat zelfde geldt voor gebruik in het kader van 'high risk government decision-making':

> "Disallowed usage of our models
> We don't allow the use of our models for the following: […]
>
> Political campaigning or lobbying, by:
> Generating high volumes of campaign materials
> Generating campaign materials personalized to or targeted at specific demographics
> Building conversational or interactive systems such as chatbots that provide information about campaigns or engage in political advocacy or lobbying
> Building products for political campaigning or lobbying purposes
>
> [...]
>
> High risk government decision-making, including:
> Law enforcement and criminal justice
> Migration and asylum" - bron: https://openai.com/policies/usage-policies)

7.21 De terms of use van Midjourney (21 juli 2023) maken daarnaast duidelijk dat personen die gebruikmaken van hun generatieve AI-tool ten behoeve van een onderneming met meer dan "$1,000,000 USD a year in gross revenue", verplicht zijn een "Pro" of "Mega" membership af te sluiten. Doen zij dat niet, dan kunnen zij geen beroep doen op de in de gebruiksvoorwaarden neergelegde eigendomsafspraken:

> "If You are an employee or owner of a company with more than $1,000,000 USD a year in gross revenue and You are using the Services on behalf of Your employer, You must purchase a "Pro" or "Mega" membership for every individual accessing the Services on Your behalf in order to own Assets You create. If You are not sure whether Your use qualifies as on behalf of Your employer, please assume it does." - bron: https://docs.midjourney.com/docs/terms-of-service

[33] Zie voor de volledige voorwaarden: https://openai.com/policies/sharing-publication-policy

7.22 Noemenswaardig is bovendien dat dezelfde gebruiksvoorwaarden ook bepalen dat Midjourney een eeuwigdurend, wereldwijd, royaltyvrije, niet-opzegbare, sub-licentieerbare, niet-exclusieve licentie ontvangt op alle input die bij hen door een gebruiker wordt aangeleverd:

> "By using the Services, You grant to Midjourney, its successors, and assigns a perpetual, worldwide, non-exclusive, sublicensable no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute text, and image prompts You input into the Services, or Assets produced by the service at Your direction. This license survives termination of this Agreement by any party, for any reason."

Auteursrechtelijke risico's Staat als (werkgever van) eindgebruiker

7.23 Uit het voorgaande volgt niet dat het gebruik van generatieve AI-tools door de Staat als werkgever op grond van het auteursrecht categoraal onrechtmatig is. Door medewerkers van de Staat toe te staan van dergelijke tools gebruik te laten maken, ontstaan in theorie wel auteursrechtelijke risico's waarvan de precieze omvang niet goed valt in te schatten. De Staat heeft meerdere mogelijkheden daarmee om te gaan.

7.24 De meest risico vermijdende keuze is ervoor te kiezen vooralsnog in het geheel geen gebruik te maken van generatieve AI-tools, in afwachting van verduidelijkende regelgeving of rechtspraak, of in afwachting van transparantieverplichtingen die gebruikers in staat stellen na te gaan of de betreffende dienst auteursrechten van derden voldoende respecteert en of gegenereerde output geen inbreuk maakt op rechten van derden.

7.25 Een andere mogelijkheid is dat de Staat het gebruik van bepaalde generatieve AI-tools binnen bepaalde grenzen, en ten behoeve van duidelijk afgebakende doelstellingen of werkzaamheden, toestaat. Dit stelt de Staat in staat ervoor te waken dat geen gebruik wordt gemaakt van generatieve AI-tools waarvan de gebruiksrichtlijnen of algemene voorwaarden bepalingen bevatten die voor de Staat onaanvaardbare risico's in het leven roepen (zoals bijvoorbeeld op het gebied van vrijwaring), of die gebruik voor overheidsdoeleinden in het geheel niet toestaan. Het risico dat de Staat aansprakelijk wordt gesteld voor het gebruiken van een dienst die inbreuk maakt op auteursrechten, of dat het gebruik van gegenereerde output in incidentele gevallen tot aansprakelijkheid leidt, blijft dan bestaan. Tegelijkertijd wordt dat risico deels gemitigeerd.

> Wij merken daarbij op dat de Staat uiteraard ook met leveranciers van AI-tools (zoals bijvoorbeeld Microsoft) in gesprek kan treden, onder meer over het bieden van de garantie dat het gebruik van een AI-tool niet leidt tot inbreuk op rechten van derden.

7.26 Flankerend aan laatstgenoemde mogelijkheid zou de Staat interne richtlijnen kunnen introduceren die het gebruik van generatieve AI-tools door medewerkers van de Staat verder vormgeven. Daarbij kan (bijvoorbeeld) aansluiting worden gezocht bij de (equivalente) interne guidelines gebruik van generatieve AI-tools die de Europese Commissie voor medewerkers heeft opgesteld. Gemakshalve voegen wij deze guidelines als **bijlage** bij dit advies.

7.27 De guidelines bevatten verschillende regels waaraan medewerkers van de Europese Commissie zich bij het gebruik van generatieve AI-tools dienen te houden. Daarbij stellen de guidelines voorop dat, zoals hiervoor werd besproken, bij de ontwikkeling van AI-tools gebruik kan zijn gemaakt van beschermd materiaal, waardoor (ook bij het gebruik van de uiteindelijke output) sprake kan zijn van auteursrechtschendingen. Gecombineerd met het feit dat de algemene voorwaarden van aanbieders van AI-tools veelal de aansprakelijkheid uitsluiten, leidt dit tot de interne regel dat:

> "Staff should always critically assess whether the outputs of an online available generative AI model are not violating intellectual property rights, in particular copyright of third parties", waarbij medewerkers voor advies terecht kunnen bij een interne Afdeling op het gebied van intellectuele-eigendom,

en de regel dat:

> "Staff shall never directly replicate the output of a generative AI model in public documents, such as the creation of Commission texts, notably legally binding ones".

7.28 De guidelines bevatten daarnaast onder meer een algeheel verbod om persoonsgegevens of (andere) informatie die zich niet al in het publieke domein bevindt met generatieve AI-tools te delen, en een verplichting alert te zijn op mogelijke biases en feitelijk onjuiste informatie.

7.29 Wij raden aan om, als besloten wordt het gebruik van generatieve AI-tools door medewerkers van de Staat (binnen nader te bepalen grenzen) toe te staan, in ieder geval ook de in de guidelines van de Europese Commissie genoemde regels (of regels van gelijke strekking) van toepassing te verklaren. Voor het overige zijn wij graag bereid met u in overleg te treden over de mogelijkheid eventuele nadere regels of voorwaarden aan het beoogde gebruik te verbinden.

8 Overige regelgeving

AI Act

8.1 Hoewel de AVG en de EU Artificial Intelligence Act (AI Act) ogenschijnlijk op veel punten overlappen, is het belangrijk om vast te stellen dat ze verschillende regelgevingsdoelen dienen.

8.2 De AVG is technologie neutraal geformuleerd en verwijst niet expliciet naar specifieke technologische toepassingen (waaronder AI of machine learning), maar richt zich uitsluitend op persoonsgegevens. Aan de andere kant hanteert de AI Act een meer directe, praktijkgerichte benadering van AI-regulering en probeert deze een alomvattend regelgevingskader vast te stellen om de verantwoorde ontwikkeling, en het verantwoorde gebruik, van op AI gebaseerde systemen in de EU te bevorderen.

Afwijkende normadressaat

8.3 Verder is van belang dat de AI Act een andere normadressaat kent dan de AVG. In plaats van zich te richten op de rol van de partijen met betrekking tot de verwerking van persoonsgegevens, richt het voorstel voor de AI Act zich op de organisaties die AI-systemen voor commerciële doeleinden ontwikkelen, en op de markt brengen of gebruiken, d.w.z. respectievelijk 'aanbieders' en 'gebruikers'. Aan elk van hen worden specifieke verplichtingen opgelegd, maar het grootste deel wordt gelegd bij de aanbieders, met name als het gaat om AI-systemen met een hoog risico (HRAIS).

8.4 Deze manier om de belangrijkste actoren te definiëren, kan leiden tot inconsistentie met de definities uit de AVG. Dit heeft er toe geleid dat de EDPB en de EDPS hebben gevraagd ervoor te zorgen dat de verplichtingen van de AI Act consistent zijn met de rollen van verwerkingsverantwoordelijke en verwerker als het gaat om de verwerking van persoonsgegevens.

Verwijzing naar AVG in AI Act

8.5 In het voorstel voor de AI Act wordt reeds al verwezen naar de bepalingen uit de AVG. De voorgestelde AI Act verwijst herhaaldelijk naar de AVG, met inbegrip van de beginselen ervan, en benadrukt dat deze moeten worden ingebed in AI-systemen (overweging 45a van de AI Act).

8.6 Een voorbeeld is de grondslag die wordt verleend aan aanbieders om speciale categorieën gegevens te verwerken die vallen onder artikel 9, lid 1, en artikel 10 AVG bij het monitoren, opsporen en corrigeren van vooroordelen met betrekking tot HRAIS (artikel 10, vijfde lid, AI Act).

8.7 Daarnaast hebben aanbieders op grond van artikel 13 AI Act uitgebreide transparantieverplichtingen tegenover hun klanten (d.w.z. "gebruikers" en AVG-"verwerkingsverantwoordelijken "), teneinde laatstgenoemden in staat te stellen de output van het systeem te interpreteren en op passende wijze te gebruiken.

8.8 Deze transparantie komt in de vorm van gebruiksaanwijzingen die onder andere het beoogde doel van het HRAIS, het nauwkeurigheidsniveau, de prestaties, specificaties voor invoergegevens en geïmplementeerde maatregelen voor menselijk toezicht (zoals beschreven in artikel 14 van de AI Act) moeten specificeren.

8.9 De AI Act verwijst hierbij naar de AVG, door aan gebruikers de verplichting te stellen de informatie uit de HRAIS-gebruiksinstructies van aanbieders te gebruiken bij het uitvoeren van de DPIA in het kader van de AVG (artikel 29, zesde lid, AI Act).

8.10 Ongeacht de formulering in artikel 29, zesde lid, AI Act, kunnen gebruikers de informatie die zij hebben verkregen van aanbieders op grond van artikel 13 van de AI Act en de technische documentatie van de HRAIS niet alleen gebruiken om te voldoen aan hun plicht om een DPIA uit te voeren, maar ook om te zorgen voor een bredere afstemming op de AVG en de transparantievereisten daarvan. Dergelijke informatie kan ook nuttig zijn om te voldoen aan andere AVG-verplichtingen, bijvoorbeeld het aanvullen van hun gegevensverwerkingsactiviteiten onder artikel 30 AVG.

8.11 Er moet echter worden opgemerkt dat volgens het voorstel van de AI Act aanbieders alleen verplichtingen hebben met betrekking tot HRAIS, terwijl de hierboven genoemde verplichtingen van gebruikers/verwerkingsverantwoordelijken onder de AVG ook van toepassing kunnen zijn als de onderliggende AI-systemen niet als zodanig kwalificeren.

Telecommunicatiewet

8.12 Per 1 maart 2022 is de Wet van 16 februari 2022 tot wijziging van de Telecommunicatiewet in verband met de implementatie van Richtlijn (EU) 2018/1972 (de Telecomcode) in werking getreden. Het belangrijkste doel van de Telecomcode is het verbeteren van de randvoorwaarden voor het realiseren van snelle digitale communicatieverbindingen (connectiviteit) in de EU. De wet introduceert een uitbreiding van de reeds bestaande telecomregels naar nummeronafhankelijke interpersoonlijke (ook wel 'over the top' (OTT)) communicatiediensten, zoals WhatsApp. Op deze diensten zijn sindsdien de privacyregels, neergelegd in de Telecommunicatiewet (met name hoofdstuk 11), van toepassing. Gedacht kan bijvoorbeeld worden aan de zorg- en meldplicht rondom beveiliging (conform artikelen 11a.1 en 11a.2 van de Telecommunicatiewet).

8.13 Artikel 2 van de Telecomcode definieert een nummeronafhankelijke interpersoonlijke communicatiedienst (OTT-dienst) als volgt:

> 7) „nummeronafhankelijke interpersoonlijke communicatiedienst": een interpersoonlijke communicatiedienst die geen verbinding maakt met openbaar toegewezen nummervoorraden, namelijk een nummer of een aantal nummers

> in nationale of internationale nummerplannen, of die geen communicatie mogelijk maakt met een nummer of een aantal nummers in nationale of internationale nummerplannen;

8.14 In datzelfde artikel wordt interpersoonlijke communicatiedienst als volgt gedefinieerd;

> 5) „interpersoonlijke communicatiedienst”: een gewoonlijk tegen vergoeding aangeboden dienst die directe persoonlijke en interactieve uitwisseling van informatie via elektronischecommunicatienetwerken [sic] tussen een eindig aantal personen mogelijk maakt, waarbij de personen die de communicatie starten of eraan deelnemen, bepalen welke de ontvangers zijn, en die geen diensten omvat die persoonlijke en interactieve communicatie mogelijk maken als een louter bijkomstig kenmerk dat onlosmakelijk verbonden is met een andere dienst;

8.15 Gelet op de voornoemde definitie van OTT-diensten, lijken de meeste online beschikbare GenAI-toepassing niet als OTT-dienst te kwalificeren. Dit omdat, veelal geen sprake is van interactieve uitwisseling van informatie tussen personen. De uitwisseling van informatie die plaatsvindt bij het gebruik van GenAI is een uitwisseling van informatie tussen mens en machine, en omvat niet persoonlijke en interactieve communicatie tussen personen (interpersoonlijke communicatie).

DSA

8.16 De DSA is, net als de AI-wet, van toepassing op diensten die worden aangeboden aan gebruikers in de EU, ongeacht waar die aanbieders zijn gevestigd (artikel 2, lid 1, en artikel 3, onder d, en e, DSA).

8.17 De DSA is erop gericht om schadelijke online uitingen, zoals haatzaaien, nepnieuws of manipulatieve inhoud, te beperken. Platforms die onder de DSA vallen, zoals Facebook of X, moeten bijvoorbeeld een meldings- en actiesysteem opzetten waarmee gebruikers mogelijk illegale inhoud kunnen markeren, die vervolgens door het platform moet worden beoordeeld en, als deze illegaal wordt geacht, moet worden verwijderd (artikel 16 DSA).

8.18 Grotere platforms moeten een volledig intern klachten- en verhaalsysteem implementeren (artikel 20 DSA) en buitengerechtelijke geschillenbeslechting aanbieden (artikel 21 DSA), zodat gebruikers niet naar de rechter hoeven te stappen om content aan te vechten. erge grote online platforms moeten bovendien een volwaardig nalevingssysteem opzetten, dat onder andere bestaat uit proactieve risicobeheerstrategieën en onafhankelijke audits (artikelen 33-37 DSA).

8.19 De DSA is alleen van toepassing op zogenaamde intermediaire diensten (artikel 2, leden 1 en 2, DSA). Deze worden gedefinieerd in artikel 3, onder g DSA. Onder de

definitie vallen internet access-providers, cachingdiensten en "hosting"-diensten zoals sociale mediaplatforms.

8.20 Het is duidelijk dat de meeste GenAI-toepassing niet onder deze twee categorieën vallen. Hostingdiensten komen het dichtst in de buurt, maar zij vereisen de opslag van informatie die door, en op verzoek van, een gebruiker wordt verstrekt (artikel 3, onder g), punt iii), DSA).

8.21 Cruciaal is dat bij GenAI-toepassingen de betreffende gegevens niet door de gebruiker worden verstrekt, maar door het Gen-Ai-model zelf (nadat de gebruiker hierom heeft gevraagd door bepaalde zoektermen in te voeren (bijv. "schrijf een essay over EU-wetgeving in een juridische stijl").

8.22 In het kader van GenAI is de enige actie waarop de DSA van toepassing kan zijn, het geautomatiseerd posten van gegenereerde inhoud op traditionele sociale netwerken.

WPG

8.23 De Wet politiegegevens (hierna: Wpg) creëert voor het verwerken van politiegegevens ten behoeve van de uitvoering van de politietaak een gesloten systeem: het WPG-domein dat bestaat uit voor de verwerking van politiegegevens geautoriseerde ambtenaren van politie.

8.24 De Wpg onderscheidt verschillende grondslagen waarvoor politiegegevens mogen worden verwerkt. Deze staan in de artikelen 8, 9, 10, 12 en 13 Wpg.

8.25 Politiegegevens die verwerkt worden in het kader van de dagelijkse opsporingstaak, vallen onder artikel 8 van de Wpg. Artikel 9 maakt het mogelijk om gegevens te verwerken die specifiek gericht zijn op bepaalde personen of concrete gebeurtenissen. Het gaat hier bijvoorbeeld om onderzoeken waarbij bijzondere opsporingsbevoegdheden worden ingezet. Politiegegevens kunnen op grond van artikel 10 WPg gericht worden verwerkt met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij, kort gezegd, het beramen van misdrijven.

8.26 Artikel 13 biedt de mogelijkheid om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9 Wpg verder te verwerken voor zover dat relevant is voor:

> a. het vaststellen van eerdere verwerkingen ten aanzien van eenzelfde persoon of zaak, onder meer ter bepaling van eerdere betrokkenheid bij strafbare feiten;
> b. het ophelderen van strafbare feiten die nog niet herleid konden worden tot een verdachte;
> c. identificatie van personen of zaken;

d. het onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling danwel met het oog op een juiste bejegening van personen;
e. het uitvoeren van taken ten dienste van de justitie.

8.27 Voor het uitwisselen van politiegegevens binnen dit WPG-domein reserveert de WPG de terminologie het ter beschikking stellen van politiegegevens. Dit is beschreven in artikel 15 van de Wpg Van het verstrekken van politiegegevens wordt gesproken als politiegegevens buiten het WPG-domein worden gebracht om voor buiten de politietaak gelegen doeleinden te worden gebruikt.

8.28 Iedereen die over politiegegevens beschikt, is verplicht tot geheimhouding. De uitzonderingen op deze geheimhoudingsplicht staan beschreven in paragraaf 3 van de Wpg. In het gesloten stelsel van de Wpg is ook vastgelegd aan welke partijen buiten het Wpg-domein gegevens mogen worden verstrekt.

8.29 Als gegevens verstrekt worden, reist de geheimhoudingsplicht mee. Ze vallen na verstrekking vaak onder de AVG. De ontvanger mag de gegevens alleen verwerken voor het doel waarvoor hij ze verkregen heeft en verder geldt nog steeds de geheimhoudingsplicht.

8.30 Gelet op het gesloten stelsel van de Wpg is het verwerken van politiegegevens aan de hand van GenAI-toepassing sterk af te raden.